
**ID:** 513241
**Sample Name:** 8PRjJeUifB
**Cookbook:**
defaultlinuxfilecookbook.jbs
**Time:** 23:38:44
**Date:** 01/11/2021
**Version:** 34.0.0 Boulder Opal

# Table of Contents

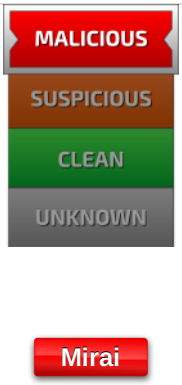
# Linux Analysis Report 8PRjJeUifB

## Overview

### General Information

| | |
|---|---|
| Sample Name: | 8PRjJeUifB |
| Analysis ID: | 513241 |
| MD5: | 0edbe8b6af0b271. |
| SHA1: | a22440162f3d3e6. |
| SHA256: | 6d1237a9ce1346.. |
| Tags: | 32 elf mips mirai |
| Infos: | |

### Detection

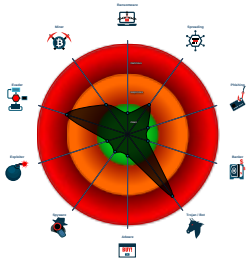



| | |
|---|---|
| Score: | 92 |
| Range: | 0 - 100 |
| Whitelisted: | false |

### Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Malicious sample detected (through ...
- Sample deletes itself
- Reads system files that contain reco...
- Sample reads /proc/mounts (often u...
- Reads CPU information from /sys in...
- Yara signature match
- Executes the "grep" command used...
- Reads system information from the ...

### Classification



### Analysis Advice

**All HTTP servers contacted by the sample do not answer. Likely the sample is an old dropper which does no longer work**

**Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures**

**Static ELF header machine description suggests that the sample might not execute correctly on this machine**

## General Information

| | |
|---|---|
| Joe Sandbox Version: | 34.0.0 Boulder Opal |
| Analysis ID: | 513241 |
| Start date: | 01.11.2021 |
| Start time: | 23:38:44 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 6m 3s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | 8PRjJeUifB |
| Cookbook file name: | defaultlinuxfilecookbook.jbs |
| Analysis system description: | Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11) |
| Analysis Mode: | default |
| Detection: | MAL |
| Classification: | mal92.troj.evad.lin@0/108@0/0 |
| Warnings: | Show All |

## Process Tree

- **system is lnxubuntu20**
- 8PRjJeUifB (PID: 5305, Parent: 5181, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/8PRjJeUifB
  - 8PRjJeUifB New Fork (PID: 5309, Parent: 5305)
  - 8PRjJeUifB New Fork (PID: 5310, Parent: 5305)
  - 8PRjJeUifB New Fork (PID: 5312, Parent: 5305)
- systemd New Fork (PID: 5316, Parent: 1)
- journalctl (PID: 5316, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --smart-relinquish-var

- systemd New Fork (PID: 5327, Parent: 1)
  - systemd-journald (PID: 5327, Parent: 1, MD5: 474667ece6cecb5e04c6eb897a1d0d9e) Arguments: /lib/systemd/systemd-journald
- systemd New Fork (PID: 5334, Parent: 1)
  - journalctl (PID: 5334, Parent: 1, MD5: bf3a987344f3bacafc44efd882abda8b) Arguments: /usr/bin/journalctl --flush
- gdm3 New Fork (PID: 5364, Parent: 1320)
  - Default (PID: 5364, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5380, Parent: 1320)
  - Default (PID: 5380, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5387, Parent: 1860)
  - pulseaudio (PID: 5387, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5395, Parent: 1)
  - accounts-daemon (PID: 5395, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
    - accounts-daemon New Fork (PID: 5409, Parent: 5395)
    - language-validate (PID: 5409, Parent: 5395, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8
      - language-validate New Fork (PID: 5410, Parent: 5409)
      - language-options (PID: 5410, Parent: 5409, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options
        - language-options New Fork (PID: 5413, Parent: 5410)
        - sh (PID: 5413, Parent: 5410, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
          - sh New Fork (PID: 5414, Parent: 5413)
          - locale (PID: 5414, Parent: 5413, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
          - sh New Fork (PID: 5415, Parent: 5413)
          - grep (PID: 5415, Parent: 5413, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -F .utf8
- gdm-session-worker New Fork (PID: 5405, Parent: 1809)
  - Default (PID: 5405, Parent: 1809, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PostSession/Default
- gdm3 New Fork (PID: 5416, Parent: 1320)
  - gdm-session-worker (PID: 5416, Parent: 1320, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
    - gdm-session-worker New Fork (PID: 5425, Parent: 5416)
    - gdm-wayland-session (PID: 5425, Parent: 5416, MD5: d3def63cf1e83f7fb8a0f13b1744ff7c) Arguments: /usr/lib/gdm3/gdm-wayland-session "dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart"
      - gdm-wayland-session New Fork (PID: 5430, Parent: 5425)
      - dbus-run-session (PID: 5430, Parent: 5425, MD5: 245f3ef6a268850b33b0225a8753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
        - dbus-run-session New Fork (PID: 5431, Parent: 5430)
        - dbus-daemon (PID: 5431, Parent: 5430, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --nofork --print-address 4 --session
          - dbus-daemon New Fork (PID: 5437, Parent: 5431)
            - dbus-daemon New Fork (PID: 5438, Parent: 5437)
            - false (PID: 5438, Parent: 5437, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5440, Parent: 5431)
            - dbus-daemon New Fork (PID: 5441, Parent: 5440)
            - false (PID: 5441, Parent: 5440, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5442, Parent: 5431)
            - dbus-daemon New Fork (PID: 5443, Parent: 5442)
            - false (PID: 5443, Parent: 5442, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5444, Parent: 5431)
            - dbus-daemon New Fork (PID: 5445, Parent: 5444)
            - false (PID: 5445, Parent: 5444, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5446, Parent: 5431)
            - dbus-daemon New Fork (PID: 5447, Parent: 5446)
            - false (PID: 5447, Parent: 5446, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5448, Parent: 5431)
            - dbus-daemon New Fork (PID: 5449, Parent: 5448)
            - false (PID: 5449, Parent: 5448, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
          - dbus-daemon New Fork (PID: 5451, Parent: 5431)
            - dbus-daemon New Fork (PID: 5452, Parent: 5451)
            - false (PID: 5452, Parent: 5451, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-run-session New Fork (PID: 5434, Parent: 5430)
        - gnome-session (PID: 5434, Parent: 5430, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: gnome-session --autostart /usr/share/gdm/greeter/autostart
        - gnome-session-binary (PID: 5434, Parent: 5430, MD5: d9b90be4f7db60cb3c2d3da6a1d31bfb) Arguments: /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
          - gnome-session-binary New Fork (PID: 5453, Parent: 5434)
          - session-migration (PID: 5453, Parent: 5434, MD5: 5227af42ebf14ac2fe2acddb002f68dc) Arguments: session-migration
          - gnome-session-binary New Fork (PID: 5454, Parent: 5434)
          - sh (PID: 5454, Parent: 5434, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell
          - gnome-shell (PID: 5454, Parent: 5434, MD5: da7a257239677622fe4b3a65972c9e87) Arguments: /usr/bin/gnome-shell
- gdm3 New Fork (PID: 5417, Parent: 1320)
  - Default (PID: 5417, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5479, Parent: 1320)
  - gdm-session-worker (PID: 5479, Parent: 1320, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
    - gdm-session-worker New Fork (PID: 5484, Parent: 5479)
    - gdm-x-session (PID: 5484, Parent: 5479, MD5: 498a824333f1c1ec7767f4612d1887cc) Arguments: /usr/lib/gdm3/gdm-x-session "dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart"
      - gdm-x-session New Fork (PID: 5486, Parent: 5484)
      - Xorg (PID: 5486, Parent: 5484, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/bin/Xorg vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeptty -verbose 3
      - Xorg.wrap (PID: 5486, Parent: 5484, MD5: 48993830888200ecf19dd7def0884dfd) Arguments: /usr/lib/xorg/Xorg.wrap vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeptty -verbose 3
      - Xorg (PID: 5486, Parent: 5484, MD5: 730cf4c45a7ee8bea88abf165463b7f8) Arguments: /usr/lib/xorg/Xorg vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeptty -verbose 3
        - Xorg New Fork (PID: 5519, Parent: 5486)
        - sh (PID: 5519, Parent: 5486, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "\"/usr/bin/xkbcomp\" -w 1 \"-R/usr/share/X11/xkb\" -xkm \"-\" -em1 \"The XKEYBOARD keymap compiler (xkbcomp) reports:\" -emp \"> \" -eml \"Errors from xkbcomp are not fatal to the X server\" \"/tmp/server-0.xkm\""
          - sh New Fork (PID: 5520, Parent: 5519)
          - xkbcomp (PID: 5520, Parent: 5519, MD5: c5f953aec4c00d2a1cc27acb75d62c9b) Arguments: /usr/bin/xkbcomp -w 1 -R/usr/share/X11/xkb -xkm - -em1 "The XKEYBOARD keymap compiler (xkbcomp) reports:" -emp "> " -eml "Errors from xkbcomp are not fatal to the X server" /tmp/server-0.xkm
        - Xorg New Fork (PID: 5897, Parent: 5486)
        - sh (PID: 5897, Parent: 5486, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "\"/usr/bin/xkbcomp\" -w 1 \"-R/usr/share/X11/xkb\" -xkm \"-\" -em1 \"The XKEYBOARD keymap compiler (xkbcomp) reports:\" -emp \"> \" -eml \"Errors from xkbcomp are not fatal to the X server\" \"/tmp/server-0.xkm\""
          - sh New Fork (PID: 5900, Parent: 5897)
          - xkbcomp (PID: 5900, Parent: 5897, MD5: c5f953aec4c00d2a1cc27acb75d62c9b) Arguments: /usr/bin/xkbcomp -w 1 -R/usr/share/X11/xkb -xkm - -em1 "The

XKEYBOARD keymap compiler (xkbcomp) reports:" -emp "> " -eml "Errors from xkbcomp are not fatal to the X server" /tmp/server-0.xkm

- gdm-x-session New Fork (PID: 5528, Parent: 5484)
- Default (PID: 5528, Parent: 5484, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/Prime/Default
- gdm-x-session New Fork (PID: 5529, Parent: 5484)
- dbus-run-session (PID: 5529, Parent: 5484, MD5: 245f3ef6a268850b33b0225a8753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
  - dbus-run-session New Fork (PID: 5530, Parent: 5529)
  - dbus-daemon (PID: 5530, Parent: 5529, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --nofork --print-address 4 --session
    - dbus-daemon New Fork (PID: 5546, Parent: 5530)
      - dbus-daemon New Fork (PID: 5547, Parent: 5546)
      - at-spi-bus-launcher (PID: 5547, Parent: 5546, MD5: 1563f274acd4e7ba530a55bdc4c95682) Arguments: /usr/libexec/at-spi-bus-launcher
        - at-spi-bus-launcher New Fork (PID: 5552, Parent: 5547)
        - dbus-daemon (PID: 5552, Parent: 5547, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: /usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork --print-address 3
          - dbus-daemon New Fork (PID: 6116, Parent: 5552)
            - dbus-daemon New Fork (PID: 6117, Parent: 6116)
            - at-spi2-registryd (PID: 6117, Parent: 6116, MD5: 1d904c2693452edebc7ede3a9e24d440) Arguments: /usr/libexec/at-spi2-registryd --use-gnome-session
    - dbus-daemon New Fork (PID: 5576, Parent: 5530)
      - dbus-daemon New Fork (PID: 5577, Parent: 5576)
      - false (PID: 5577, Parent: 5576, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5579, Parent: 5530)
      - dbus-daemon New Fork (PID: 5580, Parent: 5579)
      - false (PID: 5580, Parent: 5579, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5581, Parent: 5530)
      - dbus-daemon New Fork (PID: 5582, Parent: 5581)
      - false (PID: 5582, Parent: 5581, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5583, Parent: 5530)
      - dbus-daemon New Fork (PID: 5584, Parent: 5583)
      - false (PID: 5584, Parent: 5583, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5585, Parent: 5530)
      - dbus-daemon New Fork (PID: 5586, Parent: 5585)
      - false (PID: 5586, Parent: 5585, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5587, Parent: 5530)
      - dbus-daemon New Fork (PID: 5588, Parent: 5587)
      - false (PID: 5588, Parent: 5587, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5590, Parent: 5530)
      - dbus-daemon New Fork (PID: 5591, Parent: 5590)
      - false (PID: 5591, Parent: 5590, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
    - dbus-daemon New Fork (PID: 5894, Parent: 5530)
      - dbus-daemon New Fork (PID: 5895, Parent: 5894)
      - ibus-portal (PID: 5895, Parent: 5894, MD5: 562ad55bd9a4d54bd7b76746b01e37d3) Arguments: /usr/libexec/ibus-portal
    - dbus-daemon New Fork (PID: 6123, Parent: 5530)
      - dbus-daemon New Fork (PID: 6124, Parent: 6123)
      - gjs (PID: 6124, Parent: 6123, MD5: 5f3eceb792bb65c22f23d1efb4fde3ad) Arguments: /usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications
    - dbus-daemon New Fork (PID: 6185, Parent: 5530)
      - dbus-daemon New Fork (PID: 6186, Parent: 6185)
      - false (PID: 6186, Parent: 6185, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
  - dbus-run-session New Fork (PID: 5531, Parent: 5529)
  - gnome-session (PID: 5531, Parent: 5529, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: gnome-session --autostart /usr/share/gdm/greeter/autostart
  - gnome-session-binary (PID: 5531, Parent: 5529, MD5: d9b90be4f7db60cb3c2d3da6a1d31bfb) Arguments: /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
    - gnome-session-binary New Fork (PID: 5534, Parent: 5531)
    - gnome-session-check-accelerated (PID: 5534, Parent: 5531, MD5: a64839518af85b2b9de31aca27646396) Arguments: /usr/libexec/gnome-session-check-accelerated
      - gnome-session-check-accelerated New Fork (PID: 5553, Parent: 5534)
      - gnome-session-check-accelerated-gl-helper (PID: 5553, Parent: 5534, MD5: b1ab9a384f9e98a39ae5c36037dd5e78) Arguments: /usr/libexec/gnome-session-check-accelerated-gl-helper --print-renderer
      - gnome-session-check-accelerated New Fork (PID: 5563, Parent: 5534)
      - gnome-session-check-accelerated-gles-helper (PID: 5563, Parent: 5534, MD5: 1bd78885765a18e60c05ed1fb5fa3bf8) Arguments: /usr/libexec/gnome-session-check-accelerated-gles-helper --print-renderer
    - gnome-session-binary New Fork (PID: 5592, Parent: 5531)
    - session-migration (PID: 5592, Parent: 5531, MD5: 5227af42ebf14ac2fe2acddb002f68dc) Arguments: session-migration
    - gnome-session-binary New Fork (PID: 5593, Parent: 5531)
    - sh (PID: 5593, Parent: 5531, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell
    - gnome-shell (PID: 5593, Parent: 5531, MD5: da7a257239677622fe4b3a65972c9e87) Arguments: /usr/bin/gnome-shell
      - gnome-shell New Fork (PID: 5646, Parent: 5593)
      - ibus-daemon (PID: 5646, Parent: 5593, MD5: 1e00fb9860b198c73f6e364e3ff16f31) Arguments: ibus-daemon --panel disable --xim
        - ibus-daemon New Fork (PID: 5890, Parent: 5646)
        - ibus-memconf (PID: 5890, Parent: 5646, MD5: 523e939905910d06598e66385761a822) Arguments: /usr/libexec/ibus-memconf
        - ibus-daemon New Fork (PID: 5892, Parent: 5646)
          - ibus-daemon New Fork (PID: 5893, Parent: 5892)
          - ibus-x11 (PID: 5893, Parent: 1, MD5: 2aa1e54666191243814c2733d6992dbd) Arguments: /usr/libexec/ibus-x11 --kill-daemon
        - ibus-daemon New Fork (PID: 6168, Parent: 5646)
        - ibus-engine-simple (PID: 6168, Parent: 5646, MD5: 0238866d5e8802a0ce1b1b9af8cb1376) Arguments: /usr/libexec/ibus-engine-simple
    - gnome-session-binary New Fork (PID: 6140, Parent: 5531)
    - sh (PID: 6140, Parent: 5531, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sharing
    - gsd-sharing (PID: 6140, Parent: 5531, MD5: e29d9025d98590fbb69f89fdbd4438b3) Arguments: /usr/libexec/gsd-sharing
    - gnome-session-binary New Fork (PID: 6142, Parent: 5531)
    - sh (PID: 6142, Parent: 5531, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-wacom
    - gsd-wacom (PID: 6142, Parent: 5531, MD5: 13778dd1a23a4e94ddc17ac9caa4fcc1) Arguments: /usr/libexec/gsd-wacom
    - gnome-session-binary New Fork (PID: 6144, Parent: 5531)
    - sh (PID: 6144, Parent: 5531, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-color
    - gsd-color (PID: 6144, Parent: 5531, MD5: ac2861ad93ce047283e8e87cefef9a19) Arguments: /usr/libexec/gsd-color
    - gnome-session-binary New Fork (PID: 6145, Parent: 5531)
    - sh (PID: 6145, Parent: 5531, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-keyboard
    - gsd-keyboard (PID: 6145, Parent: 5531, MD5: 8e288fd17c80bb0a1148b964b2ac2279) Arguments: /usr/libexec/gsd-keyboard

- gnome-session-binary New Fork (PID: 6146, Parent: 5531)
  - sh (PID: 6146, Parent: 5531, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-print-notifications
  - gsd-print-notifications (PID: 6146, Parent: 5531, MD5: 71539698aa691718cee775d6b9450ae2) Arguments: /usr/libexec/gsd-print-notifications
    - gsd-print-notifications New Fork (PID: 6194, Parent: 6146)
      - gsd-print-notifications New Fork (PID: 6195, Parent: 6194)
        - gsd-printer (PID: 6195, Parent: 1, MD5: 7995828cf98c315fd55f2ffb3b22384d) Arguments: /usr/libexec/gsd-printer
- gnome-session-binary New Fork (PID: 6147, Parent: 5531)
  - sh (PID: 6147, Parent: 5531, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-rfkill
  - gsd-rfkill (PID: 6147, Parent: 5531, MD5: 88a16a3c0aba1759358c06215ecfb5cc) Arguments: /usr/libexec/gsd-rfkill
- gnome-session-binary New Fork (PID: 6148, Parent: 5531)
  - sh (PID: 6148, Parent: 5531, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-smartcard
  - gsd-smartcard (PID: 6148, Parent: 5531, MD5: ea1fbd7f62e4cd0331eae2ef754ee605) Arguments: /usr/libexec/gsd-smartcard
- gnome-session-binary New Fork (PID: 6150, Parent: 5531)
  - sh (PID: 6150, Parent: 5531, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-datetime
  - gsd-datetime (PID: 6150, Parent: 5531, MD5: d80d39745740de37d6634d36e344d4bc) Arguments: /usr/libexec/gsd-datetime
- gnome-session-binary New Fork (PID: 6151, Parent: 5531)
  - sh (PID: 6151, Parent: 5531, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-media-keys
  - gsd-media-keys (PID: 6151, Parent: 5531, MD5: a425448c135afb4b8bfd79cc0b6b74da) Arguments: /usr/libexec/gsd-media-keys
- gnome-session-binary New Fork (PID: 6153, Parent: 5531)
  - sh (PID: 6153, Parent: 5531, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-screensaver-proxy
  - gsd-screensaver-proxy (PID: 6153, Parent: 5531, MD5: 77e309450c87dceee43f1a9e50cc0d02) Arguments: /usr/libexec/gsd-screensaver-proxy
- gnome-session-binary New Fork (PID: 6154, Parent: 5531)
  - sh (PID: 6154, Parent: 5531, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sound
  - gsd-sound (PID: 6154, Parent: 5531, MD5: 4c7d3fb993463337b4a0eb5c80c760ee) Arguments: /usr/libexec/gsd-sound
- gnome-session-binary New Fork (PID: 6158, Parent: 5531)
  - sh (PID: 6158, Parent: 5531, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-a11y-settings
  - gsd-a11y-settings (PID: 6158, Parent: 5531, MD5: 18e243d2cf30ecee7ea89d1462725c5c) Arguments: /usr/libexec/gsd-a11y-settings
- gnome-session-binary New Fork (PID: 6161, Parent: 5531)
  - sh (PID: 6161, Parent: 5531, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-housekeeping
  - gsd-housekeeping (PID: 6161, Parent: 5531, MD5: b55f3394a84976ddb92a2915e5d76914) Arguments: /usr/libexec/gsd-housekeeping
- gnome-session-binary New Fork (PID: 6167, Parent: 5531)
  - sh (PID: 6167, Parent: 5531, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-power
  - gsd-power (PID: 6167, Parent: 5531, MD5: 28b8e1b43c3e7f1db6741ea1ecd978b7) Arguments: /usr/libexec/gsd-power
- gnome-session-binary New Fork (PID: 7011, Parent: 5531)
  - sh (PID: 7011, Parent: 5531, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/spice-vdagent
  - spice-vdagent (PID: 7011, Parent: 5531, MD5: 80fb7f613aa78d1b8a229dbcf4577a9d) Arguments: /usr/bin/spice-vdagent
- gnome-session-binary New Fork (PID: 7015, Parent: 5531)
  - sh (PID: 7015, Parent: 5531, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh xbrlapi -q
  - xbrlapi (PID: 7015, Parent: 5531, MD5: 0cfe25df39d38af32d6265ed947ca5b9) Arguments: xbrlapi -q
- gdm3 New Fork (PID: 5480, Parent: 1320)
  - Default (PID: 5480, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5481, Parent: 1320)
  - Default (PID: 5481, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gvfsd-fuse New Fork (PID: 5490, Parent: 2038)
  - fusermount (PID: 5490, Parent: 2038, MD5: 576a1b135c82bdcbc97a91acea900566) Arguments: fusermount -u -q -z -- /run/user/1000/gvfs
- systemd New Fork (PID: 5506, Parent: 1)
  - systemd-user-runtime-dir (PID: 5506, Parent: 1, MD5: d55f4b0847f88131dbcfb07435178e54) Arguments: /lib/systemd/systemd-user-runtime-dir stop 1000
- systemd New Fork (PID: 5618, Parent: 1)
  - systemd-localed (PID: 5618, Parent: 1, MD5: 1244af9646256d49594f2a8203329aa9) Arguments: /lib/systemd/systemd-localed
- systemd New Fork (PID: 5906, Parent: 1334)
  - pulseaudio (PID: 5906, Parent: 1334, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5907, Parent: 1)
  - geoclue (PID: 5907, Parent: 1, MD5: 30ac5455f3c598dde91dc87477fb19f7) Arguments: /usr/libexec/geoclue
- systemd New Fork (PID: 6196, Parent: 1)
  - systemd-hostnamed (PID: 6196, Parent: 1, MD5: 2cc8a5576629a2d5bd98e49a4b8bef65) Arguments: /lib/systemd/systemd-hostnamed
- systemd New Fork (PID: 6539, Parent: 1)
  - fprintd (PID: 6539, Parent: 1, MD5: b0d8829f05cd028529b84b061b660e84) Arguments: /usr/libexec/fprintd
- systemd New Fork (PID: 6746, Parent: 1)
  - systemd-localed (PID: 6746, Parent: 1, MD5: 1244af9646256d49594f2a8203329aa9) Arguments: /lib/systemd/systemd-localed
- **cleanup**

# Yara Overview

## Initial Sample

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 8PRjJeUifB | SUSP_XORed_Mozilla | Detects suspicious XORed keyword - Mozilla/5.0 | Florian Roth | • 0x16184:$xo1: \x175 366;uotj<br>• 0x161f4:$xo1: \x175 366;uotj<br>• 0x16264:$xo1: \x175 366;uotj<br>• 0x162d4:$xo1: \x175 366;uotj<br>• 0x16344:$xo1: \x175 366;uotj |

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 8PRjJeUifB | MAL_ELF_LNX_Mirai_Oct10_2 | Detects ELF malware Mirai related | Florian Roth | • 0x15d40:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 2F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A |
| 8PRjJeUifB | JoeSecurity_Mirai_5 | Yara detected Mirai | Joe Security | |

## PCAP (Network Traffic)

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| dump.pcap | JoeSecurity_Mirai_12 | Yara detected Mirai | Joe Security | |

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 5312.1.00000000c8d86b16.00000000790f233f.rw-.sdmp | SUSP_XORed_Mozilla | Detects suspicious XORed keyword - Mozilla/5.0 | Florian Roth | • 0x2284:$xo1: \x175 366;uotj<br>• 0x22f8:$xo1: \x175 366;uotj<br>• 0x236c:$xo1: \x175 366;uotj<br>• 0x23e0:$xo1: \x175 366;uotj<br>• 0x2454:$xo1: \x175 366;uotj |
| 5305.1.00000000395ac930.00000000807ae3ac.r-x.sdmp | SUSP_XORed_Mozilla | Detects suspicious XORed keyword - Mozilla/5.0 | Florian Roth | • 0x16184:$xo1: \x175 366;uotj<br>• 0x161f4:$xo1: \x175 366;uotj<br>• 0x16264:$xo1: \x175 366;uotj<br>• 0x162d4:$xo1: \x175 366;uotj<br>• 0x16344:$xo1: \x175 366;uotj |
| 5305.1.00000000395ac930.00000000807ae3ac.r-x.sdmp | MAL_ELF_LNX_Mirai_Oct10_2 | Detects ELF malware Mirai related | Florian Roth | • 0x15d40:$c01: 50 4F 53 54 20 2F 63 64 6E 2D 63 67 69 2F 00 00 20 48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 00 0D 0A 48 6F 73 74 3A |
| 5305.1.00000000395ac930.00000000807ae3ac.r-x.sdmp | JoeSecurity_Mirai_5 | Yara detected Mirai | Joe Security | |
| 5312.1.00000000395ac930.00000000807ae3ac.r-x.sdmp | SUSP_XORed_Mozilla | Detects suspicious XORed keyword - Mozilla/5.0 | Florian Roth | • 0x16184:$xo1: \x175 366;uotj<br>• 0x161f4:$xo1: \x175 366;uotj<br>• 0x16264:$xo1: \x175 366;uotj<br>• 0x162d4:$xo1: \x175 366;uotj<br>• 0x16344:$xo1: \x175 366;uotj |
| Click to see the 11 entries | | | | |

# Jbx Signature Overview

Click to jump to signature section

- AV Detection
- Bitcoin Miner
- Networking
- System Summary
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

## AV Detection:

**Multi AV Scanner detection for submitted file**

## Networking:

**Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)**

## System Summary:

**Malicious sample detected (through community Yara rule)**

## Persistence and Installation Behavior:

**Sample reads /proc/mounts (often used for finding a writable filesystem)**

## Hooking and other Techniques for Hiding and Protection:

**Sample deletes itself**

## Language, Device and Operating System Detection:

**Reads system files that contain records of logged in users**

## Stealing of Sensitive Information:

**Yara detected Mirai**

## Remote Access Functionality:

**Yara detected Mirai**

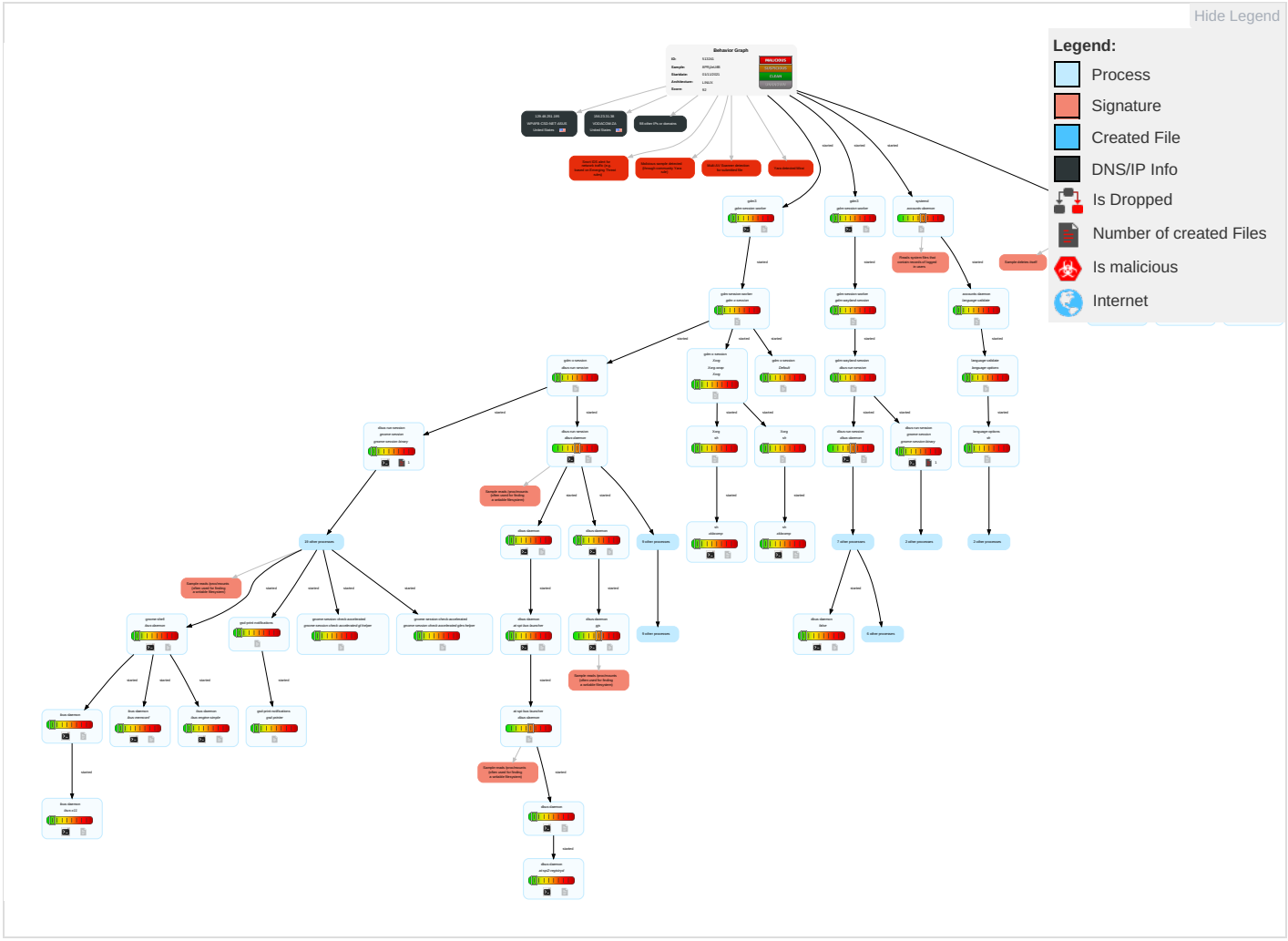
# Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impa |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Scripting 1 | Path Interception | Path Interception | File and Directory Permissions Modification 1 | OS Credential Dumping 1 | Security Software Discovery 1 1 | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | Encrypted Channel 1 | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | Modi Syst Parti |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Scripting 1 | LSASS Memory | System Owner/User Discovery 1 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Non-Standard Port 1 | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | Devi Lock |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Hidden Files and Directories 1 | Security Account Manager | File and Directory Discovery 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Application Layer Protocol 1 | Exploit SS7 to Track Device Location | Obtain Device Cloud Backups | Dele Devi Data |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Indicator Removal on Host 1 | NTDS | System Information Discovery 2 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Protocol Impersonation | SIM Card Swap | | Carri Billin Frau |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | File Deletion 1 | LSA Secrets | Remote System Discovery | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | Manipulate Device Communication | | Mani App Rank or Ra |

# Malware Configuration

**No configs have been found**

# Behavior Graph




# Antivirus, Machine Learning and Genetic Malware Detection

## Initial Sample

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| 8PRjJeUifB | 37% | Virustotal | | Browse |
| 8PRjJeUifB | 55% | ReversingLabs | Linux.Trojan.Mirai | |

## Dropped Files

No Antivirus matches

## Domains

No Antivirus matches

## URLs

No Antivirus matches

# Domains and IPs

## Contacted Domains

No contacted domains info

## URLs from Memory and Binaries

## Contacted IPs

### Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 49.238.232.212 | unknown | Korea Republic of | | 4766 | KIXS-AS-KRKoreaTelecomKR | false |
| 162.76.205.254 | unknown | United States | | 7155 | VIASAT-SP-BACKBONEUS | false |
| 207.77.249.220 | unknown | United States | | 701 | UUNETUS | false |
| 88.240.55.173 | unknown | Turkey | | 9121 | TTNETTR | false |
| 100.210.236.0 | unknown | United States | | 21928 | T-MOBILE-AS21928US | false |
| 172.143.38.246 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 128.146.245.196 | unknown | United States | | 159 | OSUNET-ASUS | false |
| 211.242.81.217 | unknown | Korea Republic of | | 9457 | DREAMX-ASDREAMLINECOKR | false |
| 79.142.84.154 | unknown | Russian Federation | | 8492 | OBIT-ASOBITLtdRU | false |
| 183.32.34.91 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 63.207.221.209 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 170.49.43.69 | unknown | United States | | 14017 | BNSF-ASUS | false |
| 67.191.151.143 | unknown | United States | | 7922 | COMCAST-7922US | false |
| 221.136.234.207 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 67.222.180.254 | unknown | United States | | 54119 | BOINGO-MDUUS | false |
| 1.200.209.231 | unknown | Taiwan; Republic of China (ROC) | | 24157 | VIBO-NET-ASTaiwanStarTelecomCorporationLimitedFormer | false |
| 151.241.96.245 | unknown | Iran (ISLAMIC Republic Of) | | 31549 | RASANAIR | false |
| 76.210.212.67 | unknown | United States | | 7018 | ATT-INTERNET4US | false |
| 203.61.203.118 | unknown | Australia | | 703 | UUNETUS | false |
| 194.75.157.161 | unknown | United Kingdom | | 32787 | PROLEXIC-TECHNOLOGIES-DDOS-MITIGATION-NETWORKUS | false |
| 208.197.203.108 | unknown | United States | | 701 | UUNETUS | false |
| 67.97.52.119 | unknown | United States | | 6977 | IAC-ASUS | false |
| 94.66.233.224 | unknown | Greece | | 6799 | OTENET-GRAthens-GreeceGR | false |
| 93.169.118.181 | unknown | Saudi Arabia | | 39891 | ALJAWWALSTC-ASSA | false |
| 222.59.175.56 | unknown | China | | 9394 | CTTNETChinaTieTongTelecommunicationsCorporationCN | false |
| 76.87.9.117 | unknown | United States | | 20001 | TWC-20001-PACWESTUS | false |
| 105.241.148.121 | unknown | South Africa | | 37457 | Telkom-InternetZA | false |
| 175.47.19.212 | unknown | China | | 17968 | DQTNETDaqingzhongjipetroleumtelecommunicationconstructi | false |
| 14.209.130.210 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 136.135.17.205 | unknown | United States | | 60311 | ONEFMCH | false |
| 129.48.251.195 | unknown | United States | | 132 | WPAFB-CSD-NET-ASUS | false |
| 143.102.96.231 | unknown | United States | | 13636 | NEC-LABORATORIES-AMERICA-INCUS | false |
| 45.216.221.197 | unknown | Morocco | | 36925 | ASMediMA | false |
| 41.71.222.26 | unknown | Nigeria | | 37053 | RSAWEB-ASZA | false |
| 39.203.199.128 | unknown | Indonesia | | 23693 | TELKOMSEL-ASN-IDPTTelekomunikasiSelularID | false |
| 170.131.193.32 | unknown | United States | | 13954 | STAPLESUS | false |
| 144.174.107.222 | unknown | United States | | 2553 | FSU-ASUS | false |
| 40.155.56.114 | unknown | United States | | 4249 | LILLY-ASUS | false |
| 94.49.43.24 | unknown | Saudi Arabia | | 25019 | SAUDINETSTC-ASSA | false |
| 93.180.103.228 | unknown | Bosnia and Herzegowina | | 42560 | BA-TELEMACH-ASTelemachdooSarajevoBA | false |
| 178.185.114.231 | unknown | Russian Federation | | 12389 | ROSTELECOM-ASRU | false |
| 201.223.155.213 | unknown | Chile | | 7418 | TELEFONICACHILESACL | false |
| 84.192.134.53 | unknown | Belgium | | 6848 | TELENET-ASBE | false |

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 176.80.242.237 | unknown | Spain | | 3352 | TELEFONICA_DE_ESPANA ES | false |
| 97.255.238.5 | unknown | United States | | 6167 | CELLCO-PARTUS | false |
| 14.36.136.20 | unknown | Korea Republic of | | 4766 | KIXS-AS-KRKoreaTelecomKR | false |
| 207.225.240.242 | unknown | United States | | 209 | CENTURYLINK-US-LEGACY-QWESTUS | false |
| 175.44.166.81 | unknown | China | | 4837 | CHINA169-BACKBONECHINAUNICOM China169BackboneCN | false |
| 209.51.148.138 | unknown | United States | | 11042 | NTHLUS | false |
| 155.206.126.243 | unknown | United States | | 6629 | NOAA-ASUS | false |
| 52.243.103.120 | unknown | United States | | 8075 | MICROSOFT-CORP-MSN-AS-BLOCKUS | false |
| 189.215.177.136 | unknown | Mexico | | 28509 | CablemasTelecomunicacionesSAdeCVMX | false |
| 27.61.234.172 | unknown | India | | 45609 | BHARTI-MOBILITY-AS-APBhartiAirtelLtdASforGPRS Service | false |
| 25.149.132.121 | unknown | United Kingdom | | 7922 | COMCAST-7922US | false |
| 42.237.49.239 | unknown | China | | 4837 | CHINA169-BACKBONECHINAUNICOM China169BackboneCN | false |
| 201.111.91.66 | unknown | Mexico | | 8151 | UninetSAdeCVMX | false |
| 184.27.119.125 | unknown | United States | | 20940 | AKAMAI-ASN1EU | false |
| 99.221.167.194 | unknown | Canada | | 812 | ROGERS-COMMUNICATIONSCA | false |
| 191.237.130.98 | unknown | Brazil | | 8075 | MICROSOFT-CORP-MSN-AS-BLOCKUS | false |
| 162.166.121.52 | unknown | United States | | 21928 | T-MOBILE-AS21928US | false |
| 100.197.19.74 | unknown | United States | | 21928 | T-MOBILE-AS21928US | false |
| 65.252.105.127 | unknown | United States | | 701 | UUNETUS | false |
| 169.240.5.204 | unknown | United States | | 47024 | THE-METROHEALTH-SYSTEMUS | false |
| 102.233.173.121 | unknown | unknown | | 36926 | CKL1-ASNKE | false |
| 23.215.231.243 | unknown | United States | | 16625 | AKAMAI-ASUS | false |
| 92.18.133.105 | unknown | United Kingdom | | 13285 | OPALTELECOM-ASTalkTalkCommunications LimitedGB | false |
| 40.53.45.55 | unknown | United States | | 4249 | LILLY-ASUS | false |
| 113.204.27.82 | unknown | China | | 4837 | CHINA169-BACKBONECHINAUNICOM China169BackboneCN | false |
| 109.13.149.28 | unknown | France | | 15557 | LDCOMNETFR | false |
| 137.247.124.247 | unknown | United States | | 367 | DNIC-ASBLK-00306-00371US | false |
| 195.49.186.168 | unknown | Russian Federation | | 42516 | SOVTEST-INTERNET-ASRU | false |
| 156.23.31.38 | unknown | United States | | 29975 | VODACOM-ZA | false |
| 101.20.236.77 | unknown | China | | 4837 | CHINA169-BACKBONECHINAUNICOM China169BackboneCN | false |
| 164.179.4.229 | unknown | United States | | 37717 | EL-KhawarizmiTN | false |
| 167.152.174.170 | unknown | United States | | 25899 | LSNETUS | false |
| 102.183.16.56 | unknown | Liberia | | 37611 | AfrihostZA | false |
| 195.189.50.158 | unknown | Ukraine | | 48503 | TELE2-KZTele2KazakhstanKZ | false |
| 162.84.87.96 | unknown | United States | | 701 | UUNETUS | false |
| 133.124.71.104 | unknown | Japan | | 2522 | PPP-EXPJapanNetworkInformationCenterJP | false |
| 133.130.112.159 | unknown | Japan | | 7506 | INTERQGMOInternetIncJP | false |
| 183.24.110.141 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 59.155.189.150 | unknown | China | | 7474 | OPTUSCOM-AS01-AUSingTelOptusPtyLtdAU | false |
| 75.243.102.181 | unknown | United States | | 22394 | CELLCOUS | false |
| 116.3.24.1 | unknown | China | | 4837 | CHINA169-BACKBONECHINAUNICOM China169BackboneCN | false |

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 183.244.153.114 | unknown | China | | 56048 | CMNET-BEIJING-APChinaMobileCommunicaitonsCorporationCN | false |
| 198.51.240.9 | unknown | United States | | 14222 | NFCU-ASUS | false |
| 180.138.28.164 | unknown | China | | 4134 | CHINANET-BACKBONENo31Jin-rongStreetCN | false |
| 153.102.59.154 | unknown | United States | | 27064 | DNIC-ASBLK-27032-27159US | false |
| 92.62.128.29 | unknown | Lithuania | | 15440 | BALTNETACustomersASLT | false |
| 177.127.242.33 | unknown | Brazil | | 22381 | MegatelecomTelecomunicacoesLtdaBR | false |
| 52.74.75.3 | unknown | United States | | 16509 | AMAZON-02US | false |
| 192.107.2.255 | unknown | United Kingdom | | 14507 | TASTE-2-ASNUS | false |
| 92.245.158.212 | unknown | France | | 48072 | ALSATIS-ASalsatiswispnetworkASFR | false |
| 73.191.255.18 | unknown | United States | | 7922 | COMCAST-7922US | false |
| 182.51.85.175 | unknown | China | | 63590 | HEBBTNHebeiBroadcastingTVNetworkCN | false |
| 195.236.51.117 | unknown | Finland | | 719 | ELISA-ASHelsinkiFinlandEU | false |
| 155.69.207.147 | unknown | Singapore | | 9419 | NTU-AS-APNanyangTechnologicalUniversitySG | false |
| 169.164.169.104 | unknown | United States | | 37611 | AfrihostZA | false |
| 135.80.164.5 | unknown | United States | | 18676 | AVAYAUS | false |
| 104.20.174.0 | unknown | United States | | 13335 | CLOUDFLARENETUS | false |

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 93.169.118.181 | b3astmode.arm7 | Get hash | malicious | Browse | |

## Domains

No context

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| KIXS-AS-KRKoreaTelecomKR | SZAYTvvY9Y | Get hash | malicious | Browse | • 121.170.84.79 |
| | ENYxttDmO1 | Get hash | malicious | Browse | • 220.119.216.237 |
| | 7DoAjWX5uZ | Get hash | malicious | Browse | • 14.50.141.105 |
| | 1Y2rsDBP9s | Get hash | malicious | Browse | • 121.140.87.2 |
| | Ko84iLip1u | Get hash | malicious | Browse | • 49.23.108.172 |
| | arH2Af5qoc | Get hash | malicious | Browse | • 121.180.26.230 |
| | t7WU0JjLAR | Get hash | malicious | Browse | • 14.88.193.68 |
| | BVBf45GBHP | Get hash | malicious | Browse | • 183.125.44.162 |
| | FGVOkw9did | Get hash | malicious | Browse | • 210.103.12.45 |
| | izTs48VpFZ | Get hash | malicious | Browse | • 121.132.164.180 |
| | I5A5LzSAql | Get hash | malicious | Browse | • 221.145.45.66 |
| | P8AVd483d7 | Get hash | malicious | Browse | • 211.226.51.74 |
| | mRQwOz6Oit | Get hash | malicious | Browse | • 59.31.250.97 |
| | Yoshi.x86 | Get hash | malicious | Browse | • 175.224.253.88 |
| | Yoshi.arm | Get hash | malicious | Browse | • 220.124.250.18 |
| | hmt31ms9Dj.exe | Get hash | malicious | Browse | • 218.38.155.210 |
| | MbfEKZoPHY.exe | Get hash | malicious | Browse | • 218.38.155.210 |
| | mipsel | Get hash | malicious | Browse | • 118.32.107.152 |
| | arm | Get hash | malicious | Browse | • 125.144.1.47 |
| | arm7-20211101-1513 | Get hash | malicious | Browse | • 118.37.22.214 |

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| UUNETUS | SZAYTvvY9Y | Get hash | malicious | Browse | • 145.4.3.12 |
| | 1Y2rsDBP9s | Get hash | malicious | Browse | • 108.3.70.173 |
| | Ko84iLip1u | Get hash | malicious | Browse | • 207.68.36.75 |
| | arH2Af5qoc | Get hash | malicious | Browse | • 152.184.188.126 |
| | t7WU0JjLAR | Get hash | malicious | Browse | • 74.96.93.66 |
| | BVBf45GBHP | Get hash | malicious | Browse | • 212.190.194.255 |
| | izTs48VpFZ | Get hash | malicious | Browse | • 212.249.217.81 |
| | I5A5LzSAql | Get hash | malicious | Browse | • 63.61.95.221 |
| | P8AVd483d7 | Get hash | malicious | Browse | • 207.27.6.12 |
| | mRQwOz6Oit | Get hash | malicious | Browse | • 63.87.79.163 |
| | u4M7XeqKtD | Get hash | malicious | Browse | • 100.49.120.232 |
| | Yoshi.arm7 | Get hash | malicious | Browse | • 68.129.175.12 |
| | Yoshi.arm | Get hash | malicious | Browse | • 208.202.59.123 |
| | mipsel | Get hash | malicious | Browse | • 71.161.139.66 |
| | arm | Get hash | malicious | Browse | • 100.37.40.69 |
| | arm7-20211101-1513 | Get hash | malicious | Browse | • 199.171.250.153 |
| | mips | Get hash | malicious | Browse | • 108.2.102.247 |
| | JjHQ8Q1weT | Get hash | malicious | Browse | • 72.87.32.120 |
| | Antisocial.x86 | Get hash | malicious | Browse | • 193.79.200.215 |
| | Antisocial.arm | Get hash | malicious | Browse | • 100.13.48.72 |
| VIASAT-SP-BACKBONEUS | gbk4XWulUo | Get hash | malicious | Browse | • 184.21.29.113 |
| | 8MPbeDAwwZ | Get hash | malicious | Browse | • 172.242.149.112 |
| | Tsunami.arm7 | Get hash | malicious | Browse | • 184.62.171.251 |
| | lQKil1R7D9 | Get hash | malicious | Browse | • 207.241.178.1 |
| | iSdOB1UKQv | Get hash | malicious | Browse | • 162.76.165.173 |
| | JuofJwjQMT | Get hash | malicious | Browse | • 75.107.8.23 |
| | HF0udkDj2N | Get hash | malicious | Browse | • 162.74.6.195 |
| | dark.arm7 | Get hash | malicious | Browse | • 184.63.30.70 |
| | vdQzjfJR0u | Get hash | malicious | Browse | • 184.21.29.107 |
| | FbdUX5aU1N | Get hash | malicious | Browse | • 162.77.107.176 |
| | KKveTTgaAAsecNNaaaa.x86 | Get hash | malicious | Browse | • 99.197.243.79 |
| | hoho.x86 | Get hash | malicious | Browse | • 184.62.171.254 |
| | DswiO5MgMN | Get hash | malicious | Browse | • 162.76.45.24 |
| | hoho.arm7 | Get hash | malicious | Browse | • 184.62.171.255 |
| | 8r3HRghvXX | Get hash | malicious | Browse | • 184.21.29.124 |
| | Tsunami.x86 | Get hash | malicious | Browse | • 184.63.30.80 |
| | jew.x86 | Get hash | malicious | Browse | • 184.63.200.94 |
| | T5BjNBDzJa | Get hash | malicious | Browse | • 162.76.45.18 |
| | 9YBEjmPn3w | Get hash | malicious | Browse | • 99.196.113.127 |
| | sora.x86 | Get hash | malicious | Browse | • 172.243.31.91 |

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

# Created / dropped Files

| /home/saturnino/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-sink | |
|---|---|
| Process: | /usr/bin/pulseaudio |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 10 |
| Entropy (8bit): | 2.9219280948873623 |
| Encrypted: | false |

| /home/saturnino/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-sink | |
|---|---|
| SSDEEP: | 3:5bkPn:pkP |
| MD5: | FF001A15CE15CF062A3704CEA2991B5F |
| SHA1: | B06F6855F376C3245B82212AC73ADED55DFE5DEF |
| SHA-256: | C54830B41ECFA1B6FBDC30397188DDA86B7B200E62AEAC21AE694A6192DCC38A |
| SHA-512: | 65EBF7C31F6F65713CE01B38A112E97D0AE64A6BD1DA40CE4C1B998F10CD3912EE1A48BB2B279B24493062118AAB3B8753742E2AF28E56A31A7AAB27DE80E7BF |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | auto_null. |

| /home/saturnino/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-source | |
|---|---|
| Process: | /usr/bin/pulseaudio |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 18 |
| Entropy (8bit): | 3.4613201402110088 |
| Encrypted: | false |
| SSDEEP: | 3:5bkrlZsXvn:pkckv |
| MD5: | 28FE6435F34B3367707BB1C5D5F6B430 |
| SHA1: | EB8FE2D16BD6BBCCE106C94E4D284543B2573CF6 |
| SHA-256: | 721A37C69E555799B41D308849E8F8125441883AB021B723FED90A9B744F36C0 |
| SHA-512: | 6B6AB7C0979629D0FEF6BE47C5C6BCC367EDD0AAE3FC973F4DE2FD5F0A819C89E7656DB65D453B1B5398E54012B27EDFE02894AD87A7E0AF3A9C5F2EB24A919 |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | auto_null.monitor. |

| /proc/5438/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A99 |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | 0 |

| /proc/5441/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A99 |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | 0 |

| /proc/5443/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |

| /proc/5443/oom_score_adj | |
|---|---|
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A<br>99 |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | <br>0 |

| /proc/5445/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A<br>99 |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | <br>0 |

| /proc/5447/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A<br>99 |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | <br>0 |

| /proc/5449/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A<br>99 |
| Malicious: | false |

| /proc/5449/oom_score_adj | |
|---|---|
| Preview: | 0 |

| /proc/5452/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A<br>99 |
| Malicious: | false |
| Preview: | 0 |

| /proc/5547/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A<br>99 |
| Malicious: | false |
| Preview: | 0 |

| /proc/5577/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A<br>99 |
| Malicious: | false |
| Preview: | 0 |

| /proc/5580/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A<br>99 |

| /proc/5580/oom_score_adj | |
|---|---|
| Malicious: | false |
| Preview: | 0 |

| /proc/5582/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A<br>99 |
| Malicious: | false |
| Preview: | 0 |

| /proc/5584/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A<br>99 |
| Malicious: | false |
| Preview: | 0 |

| /proc/5586/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A<br>99 |
| Malicious: | false |
| Preview: | 0 |

| /proc/5588/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |

| /proc/5588/oom_score_adj | |
|---|---|
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A<br>99 |
| Malicious: | false |
| Preview: | <br>0 |

| /proc/5591/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A<br>99 |
| Malicious: | false |
| Preview: | <br>0 |

| /proc/5895/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A<br>99 |
| Malicious: | false |
| Preview: | <br>0 |

| /proc/6117/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A<br>99 |
| Malicious: | false |
| Preview: | <br>0 |

| /proc/6124/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |

| /proc/6124/oom_score_adj | |
|---|---|
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A<br>99 |
| Malicious: | false |
| Preview: | <br>0 |

| /proc/6186/oom_score_adj | |
|---|---|
| Process: | /usr/bin/dbus-daemon |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:V:V |
| MD5: | CFCD208495D565EF66E7DFF9F98764DA |
| SHA1: | B6589FC6AB0DC82CF12099D1C2D40AB994E8410C |
| SHA-256: | 5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9 |
| SHA-512: | 31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A<br>99 |
| Malicious: | false |
| Preview: | <br>0 |

| /run/systemd/journal/streams/.#9:73600iPwo6Y | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 223 |
| Entropy (8bit): | 5.548380279002128 |
| Encrypted: | false |
| SSDEEP: | 3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm6ElwviSxsjs7Lbgw3:SbFuFyLVIg1BG+f+M6EO6ji4s |
| MD5: | 8F9F88B7B14AA0596970202BAE679E42 |
| SHA1: | B6D35D38027E31D210429ADE301C4A6EED20D684 |
| SHA-256: | 36472D3C670E515947253E96C4933DDD0D7DED39130E3C7E391F759C5200543B |
| SHA-512: | 20970B26555BEF4051809F9D4642A1BFB68DABC02E1D006C2FF641E939D310C7BCC1D685FB665A27BE2BDC8397EFA508661C369318ABE3A7AA7367BC13BD1E<br>F |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_<br>ID=03ee48fdf62745b9866bc871a2205010.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service. |

| /run/systemd/journal/streams/.#9:73601s9o3q0 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 223 |
| Entropy (8bit): | 5.531829832585606 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVIg1BG+f+Mu6VrWRiHY375qji4s:qgFq6g10+f+MtWRQs |
| MD5: | DAC0B58820FD7348A71AC4AF626F1BD9 |
| SHA1: | 73D1F3E639F01B3E43B89C181F544F4F1BA745E2 |
| SHA-256: | 671016A2F5CEE62C43B3E5D590E4B4396EE6006938C9849CBF9630D75369AB0F |
| SHA-512: | 6CCAB46357D283BF9805EAEFF8327998CEE43CA94DB46B7E7C0E7E28DCCF5FE708D0ABB36970A29107C847E7552EC72E9FBD30D5A7252DFAC72562A1EB5D3<br>AA |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_<br>ID=d93f5379b5b04ac1a34d122a97dd6125.IDENTIFIER=journalctl.UNIT=systemd-journal-flush.service. |

| /run/systemd/journal/streams/.#9:74811JCEMK0 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 188 |
| Entropy (8bit): | 5.3530866393272 |
| Encrypted: | false |

| /run/systemd/journal/streams/.#9:74811JCEMK0 | |
|---|---|
| SSDEEP: | 3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm/rsyHgWvDB32jshQJ:SbFuFyLVIg1BG+f+MDsy9lGjtWL0 |
| MD5: | CD06F25071A0355EC8B9A7DED8B8ECD0 |
| SHA1: | 168327F8ADECB8F4A1144D0319FFA47ECDC4B6F9 |
| SHA-256: | 41309A6598685289B04192F930A95E7869A9D1E7DC68A4ED1AADD4DE348E9789 |
| SHA-512: | 49BA162663ED5AEF7DF0143E7F51DD0A6E52BB404C9AF0564EFC58036DB18CDC45AB08AB0D8510B9928F6C870B9C0236D44055CC29313E7569DF7DAD805EE92 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=5d5979f90deb432799734c70fdd358c7.IDENTIFIER=pulseaudio. |

| /run/systemd/journal/streams/.#9:75226oHVqq2 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 195 |
| Entropy (8bit): | 5.426974557853793 |
| Encrypted: | false |
| SSDEEP: | 3:SbFVVmFyinKMsPOfvP69ms947z+h6SnLAqC+h6KV+h6CQzuxmzjpX+8mhWPWGdLs:SbFuFyLVI6g7/+BG+f+Mh+8ENGdLTjNq |
| MD5: | 0594F116C2582C933814CE8930AD301D |
| SHA1: | 3367A86950990F9E5AEBBD7B2F5B824F07B19025 |
| SHA-256: | 38FB989E318C540FC582CB45D0C69805F6619744894DCD8ADC6F9B36631CFB78 |
| SHA-512: | 3AA40B71EBB5D73BBFB16E62D1BBBFD5582CF4D77943DFA8CB913399B29FAEBF91EEED4E91DA7D667BFFD0B61787E08C51B116C6B66C05BA8DF813D296759599 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=9e760f2014894991953c7f43c64e6f20.IDENTIFIER=gdm-session-worker. |

| /run/systemd/journal/streams/.#9:75248PdGZcY | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 204 |
| Entropy (8bit): | 5.469762244957075 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVK6g7/+BG+f+MPHdIjFQMzKYA9:qgFqo6g7/+0+f+METmt9 |
| MD5: | B7F835A570B6B52B3D89617C756E8B45 |
| SHA1: | 26DA02491B4797577F8FD1AB72719B8051F44A2C |
| SHA-256: | 67A4D7DBF4F4616EFC09560F8849BF7E13CACF3DF5F0B3F93BE0C9D8205163E4 |
| SHA-512: | CAA671E0ED94DA3EAD229DB75C9B2B93D17D2F6957BB7D7B4E8EC6DCBECD8696DEDAF6B226B2B3864B43A914279515809A847B8A82013145B19EBF8AFA4D04E8 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=55afbb83a3964a50ae8d8759c8e83d31.IDENTIFIER=/usr/lib/gdm3/gdm-x-session. |

| /run/systemd/journal/streams/.#9:75249UZltNZ | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 204 |
| Entropy (8bit): | 5.479042756985325 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVI6g7/+BG+f+M8UCgTLdH22jFQMzKYA9:qgFqdg7/+0+f+M8pjETmt9 |
| MD5: | 453E2F5C104C927490BB36CC7F7237B5 |
| SHA1: | C104F19463155C5741EDD2F03011782EF73B67A4 |
| SHA-256: | 8EC58920A2A160F48DF1F29057C1A30A15A706F4D6C4F62D5F1F4D4C77685AB1 |
| SHA-512: | 38F535820C14CF021A0E2F70123D494C638BC041CB4A90E8B69A0AD20393C129240389F2F6C5107EC03FD3DDCCD034AC37F863BE9A529EDBCB822AD8481CAE9 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=64858e00e85c47d3aecfcd8771f509d8.IDENTIFIER=/usr/lib/gdm3/gdm-x-session. |

| /run/systemd/journal/streams/.#9:75305qUAi6Y | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |

| /run/systemd/journal/streams/.#9:75305qUAi6Y | |
|---|---|
| Category: | dropped |
| Size (bytes): | 237 |
| Entropy (8bit): | 5.4598402916658495 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVIg1BG+f+Mu7DmaxDWWuqjZcHuWasI6m5esI61Udr+:qgFq6g10+f+MiDPxDWUmuWap6eep6eE |
| MD5: | 65B6C4602C5FAF0844369C270474B66A |
| SHA1: | 8AFB518F703799AA33FE5142CB6E8BE6E560EB57 |
| SHA-256: | 881934678A52C7B9D6CB9EC8C034963AEB35F48789C0E1C79036B2A7F0368FC1 |
| SHA-512: | C255FFFF21FF66AC6A6A20497290642346EA7195B31DC044C0D0134BEE1C057178AAC20D9E72ADBD6DC87AC65A5258A65EFA75AF00FFCCF539422A54E7AE0D5 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=d74094ccbc66413782ef4c7e97f3d433.IDENTIFIER=systemd-user-runtime-dir.UNIT=user-runtime-dir@1000.service. |

| /run/systemd/journal/streams/.#9:75454H76Lm0 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 222 |
| Entropy (8bit): | 5.4701394855064445 |
| Encrypted: | false |
| SSDEEP: | 3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm7s5BWRM1lEbdjsicT:SbFuFyLVIg1BG+f+MwfWGlGjZcH5CHq |
| MD5: | 7615942A75D23A152FAA78F064BF0620 |
| SHA1: | 1FACFBCF716BDBC658036A430653BB747A629664 |
| SHA-256: | 5DD871E7A62074BEBE2E6E38A759E31C42914A0A54D5BAC37A6F9D86534AA2B9 |
| SHA-512: | D0E4ED0F5E138BD6B12335B2B0A3F26E1773769293918917C7684150A06A87657CB0095C10D3D4607C820A37141D1211DFFFF5C1C4A4579B5B7A1192C62679D6 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=15105cc648d34299ad62173d5bf94c95.IDENTIFIER=systemd-localed.UNIT=systemd-localed.service. |

| /run/systemd/journal/streams/.#9:76127V85kH1 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 222 |
| Entropy (8bit): | 5.371442823184031 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVIg1BG+f+M4eB3rGNYTjLTTIWTIL:qgFq6g10+f+M48GUEWEL |
| MD5: | C355E97F3DB5469522C03877D0B45844 |
| SHA1: | A4BE0BAB7506C9AECCE23E839F0F1114C67F92A5 |
| SHA-256: | EA3B3C364DBF96C6390D24972DFCBF47267B322AD4A93B68E4BEF687A2893AD0 |
| SHA-512: | 4F28BF2DF7174C06A40D7132051D2ABE184204AEB8324071251AD2C6845AB420FF720D4CBA7C9B9A99431AE2D8BCB2FB0FE9A44ADA19449D0A2FE7D349AD30 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=27e4adddf6264eda8ae6f87a0d5fd066.IDENTIFIER=accounts-daemon.UNIT=accounts-daemon.service. |

| /run/systemd/journal/streams/.#9:76201csFGb1 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 195 |
| Entropy (8bit): | 5.433359750150389 |
| Encrypted: | false |
| SSDEEP: | 3:SbFVVmFyinKMsPOdvP69ms947z+h6SnLAqC+h6KV+h6CQzuxmu0VVWSXR93ELHId:SbFuFyLVK6g7/+BG+f+MuMR1sHI+jNq |
| MD5: | CA9B8DBC5B7F22A86BD1EAF01D1A4D28 |
| SHA1: | E4206F1716802708A06AC67A1247450F035B16BA |
| SHA-256: | 6F6E0FBA276FF900E5D629AC0FE7A8DDD07C27952DEAA547563470AAD515EE96 |
| SHA-512: | 6EC79C6A61710C4C2BEE123F21298809A27D9B5AE03430923F3572367549E1D91C18F15FD3E633356AF4BA41E917662FE024CD693395CCCB599A4C155649A6DD |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=de66003722f847a6bf8c6cdeb58e179b.IDENTIFIER=gdm-session-worker. |

| /run/systemd/journal/streams/.#9:76202GqP620 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 195 |
| Entropy (8bit): | 5.412083931661278 |
| Encrypted: | false |
| SSDEEP: | 3:SbFVVmFyinKMsPOfvP69ms947z+h6SnLAqC+h6KV+h6CQzuxm/HHG+TRcBl3vK8p:SbFuFyLVI6g7/+BG+f+MO+ely8qjNq |
| MD5: | 5933E852CEA51BFB6E61A74D6A7D8189 |
| SHA1: | 340AC91C0781B2B4EA85F6950AD887709E1763F6 |
| SHA-256: | 7F764DC23854BFB15AF98E5B7BBF09F6EFC8E0D4FF78933724D200A4F946CC8E |
| SHA-512: | 4D454101F13F3C30B304235A62A7198754C95A8DECCB447E5F5464097F85B035DA81AA33A1A29E9F23C9E7D83FF1E9464F359ED10E70FAB61B1A959F79489402 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=5c5b236fe96a4d649d372bddab96bf3e.IDENTIFIER=gdm-session-worker. |

| /run/systemd/journal/streams/.#9:76268iFsTZX | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 210 |
| Entropy (8bit): | 5.497231230077583 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVK6g7/+BG+f+Mu5C9TK9jFQMzKaBu:qgFqo6g7/+0+f+MS4STmh |
| MD5: | 7161E59E71100BB0F9C047462EA5F85A |
| SHA1: | 58F30263579090AB93DF19119B7BD7515B138AC4 |
| SHA-256: | FBFD2FA020F3B0D182A483B7774649E149850591D7CEE5B39639BCE36249326A |
| SHA-512: | DCBB9AD788D82DF2B9E77925EFDFD51373816897FF814D67C5A4910397F0CA063A3D8C7B0A9334BC54E94E68724D7E63258698F3DDBA16EC83CFFAB149D18BE |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=dcf24c0a0d2a4309a86b10bae7304c59.IDENTIFIER=/usr/lib/gdm3/gdm-wayland-session. |

| /run/systemd/journal/streams/.#9:76275nkVJa2 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 210 |
| Entropy (8bit): | 5.518490246490488 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVI6g7/+BG+f+M8wJ+QDeC22jFQMzKaBu:qgFqdg7/+0+f+M8wteC2ETmh |
| MD5: | FD1361D2F9F68A5F67325FC7F544EA26 |
| SHA1: | 60A31F13582826531824A52B6D5A22A6DC0E7112 |
| SHA-256: | DD56E691C8689BBD6CA130B216568E28D667EDECF7EEC64495708D9E9AF4BFD1 |
| SHA-512: | 85FAE02F22849FB12D000E789CA83DDBADB58E237CC9EB564C6DEB82DB6D5F6CED69855A3891C02BB65E2919286E56F807E8A134183A6C10D217163E3A525FE0 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=60a6d0b3a143483c8f1ff9adc15f8942.IDENTIFIER=/usr/lib/gdm3/gdm-wayland-session. |

| /run/systemd/journal/streams/.#9:76287SkVqz2 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 190 |
| Entropy (8bit): | 5.36702698752076 |
| Encrypted: | false |
| SSDEEP: | 3:SbFVVmFyinKMsPOdvP69ms947z+h6SnLAqC+h6KV+h6CQzuxm4bDnldeQJACTjsE:SbFuFyLVK6g7/+BG+f+M4bDldeQJ1TjV |
| MD5: | 065109B8AB0364465986190A31E6873F |
| SHA1: | B0BEED5B563CE263893D3082A778BC000B1A5853 |
| SHA-256: | 347841B26D8A00E02F390309215CA1CEE29E59B7BA6C8BB398CF9D936C4ACEB9 |
| SHA-512: | 8E98AA7B4BBDEEDEDC25D654D209D531D08A8888AFE6146B69E237CD9B9C5519FC7F663093AD9E769E513E3CA0F0E5D2A3A7028E2092619555B0453B68861EEA |
| Malicious: | false |

| /run/systemd/journal/streams/.#9:76287SkVqz2 | |
|---|---|
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=29aef76f20fb46639d8c083dbfbcc6e4.IDENTIFIER=gnome-session. |

| /run/systemd/journal/streams/.#9:76370byhZh1 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 200 |
| Entropy (8bit): | 5.408009327776304 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVK6g7/+BG+f+M8ZmIqEQH928jFmzXvn:qgFqo6g7/+0+f+M8ZmIK7QXvn |
| MD5: | B5BCEF5A2266244DA272ABC6D2F2B6F0 |
| SHA1: | B8B1480455BC81E6C36A807E4EF5F2785BFBE47C |
| SHA-256: | 9F54D2C87F56092D202426EB84EBDCAAFD8AFBBA97643FDDE838C88189145C3B |
| SHA-512: | 7CAE72DB92C3240D3DF275B24708F46F6B6DF82D6219BADE5D09328E3D2BA5FCD54B77021A0A6F569900B1AE705224A91A8F09CFA6B44D90F1AAFB72DA1DBF0E |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=6e1b75d58d1945e590fa52e742912551.IDENTIFIER=org.gnome.Shell.desktop. |

| /run/systemd/journal/streams/.#9:76372YgBy71 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 200 |
| Entropy (8bit): | 5.3650380448800465 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVI6g7/+BG+f+MukLEqKI2jFmzXvn:qgFqdg7/+0+f+MzjKVQXvn |
| MD5: | 9BEEC567B04B1558F63D128E97FFC6AB |
| SHA1: | 52615145B8D51A17B69ACF559BC5A1EAACADA841 |
| SHA-256: | D1E500BCB53126461F0585EB14008CD704AEA5DE8CE1ED0CA020C04F115BE90B |
| SHA-512: | 796ECC96E741D538278C2F1A2D4902786FBE77BADD534579EF1485592AAF92DC331F3A39A522DCACFF51218B4A1D7586A389F91A0E612E7F060972D52D283D5 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=d3cad2a07e0340ae8eeb5a59a5349963.IDENTIFIER=org.gnome.Shell.desktop. |

| /run/systemd/journal/streams/.#9:76450q1sSZ0 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 195 |
| Entropy (8bit): | 5.383220357978718 |
| Encrypted: | false |
| SSDEEP: | 3:SbFVVmFyinKMsPOdvP69ms947z+h6SnLAqC+h6KV+h6CQzuxm6qoh3JCEPXGdtBe:SbFuFyLVK6g7/+BG+f+M6qeJHPX52jNq |
| MD5: | AEA9664E3855CACDA44F2C09B5E7DFA3 |
| SHA1: | 0F1CC3A9134176641185D99FA360F8AA69672C6F |
| SHA-256: | 20C83E5FD5391B0EE630F69E8D9ECEECC7EA81EACA81E959A5721199C0BE87F0 |
| SHA-512: | D0ABDEBA4483FE9A3510C1C1BC7570D798A9874FF7F8EED5F25B259774A7C4106E88A3145175B88CCD83D5AD928793EA40B4787724580846B65147C98BA6C84 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=00fa438d27a242c98eaf48293c899d03.IDENTIFIER=gdm-session-worker. |

| /run/systemd/journal/streams/.#9:76724cc4Kj0 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 190 |
| Entropy (8bit): | 5.366060916836325 |
| Encrypted: | false |
| SSDEEP: | 3:SbFVVmFyinKMsPOdvP69ms947z+h6SnLAqC+h6KV+h6CQzuxm9x45+jaUQcUX6ry:SbFuFyLVK6g7/+BG+f+Mz4bUQlKrqjNb |
| MD5: | EB414DF5C366C2E7F806A254ADB2C071 |
| SHA1: | 0C2F2D5C750653A4354D6C1FA3B6F3A49F45ABF8 |
| SHA-256: | FA6EA6D5201A3722E0F6B3F512E7FF7AEA530E6E5EFF9358FBF46760F76777EF |

| /run/systemd/journal/streams/.#9:76724cc4Kj0 | |
|---|---|
| SHA-512: | C79D6739351B06641770C2164A561776E5C868B013FA690AA1F8788AE91E77485C69D28E2F8CF6CE11E9C271296808F0E65150333A4C2B30656150BBFEE5D06F |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=7a99e4e8b30c4ecdb015101f4d15912a.IDENTIFIER=gnome-session. |

| /run/systemd/journal/streams/.#9:76863WFZi3Y | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 200 |
| Entropy (8bit): | 5.394119452333965 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVK6g7/+BG+f+Ms0yT60XqjFmzXvn:qgFqo6g7/+0+f+MpyTp4QXvn |
| MD5: | AE3809988A039846579A4EE3BFDDA6AE |
| SHA1: | F2908CD3B25B59C3AE6D108E4472E07E6240B4B2 |
| SHA-256: | 85DDE9DCF05C99AD6390D97B19A9EC37EEB9A53DC1F9845D161CD857DB739641 |
| SHA-512: | 8AD29757A546231CEA99A46F45E422F037348D19B38CE9D9A5295B78199E74161A24C4817A70EFEF000CE786767DB89D933221F9C6C09130D91FED5BCBEE8CF |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=74e6b8a0ae7d4d61adf61cea5d7b319a.IDENTIFIER=org.gnome.Shell.desktop. |

| /run/systemd/journal/streams/.#9:768656GzIPZ | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 200 |
| Entropy (8bit): | 5.442283092637671 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVl6g7/+BG+f+MOB7PcDUpjFmzXvn:qgFqdg7/+0+f+MOB7kg/QXvn |
| MD5: | 88E7852F51E7F5FC862358E7B51D4857 |
| SHA1: | 42AD1B6C0BD6250B7A0B50F32B57EB842D990BDF |
| SHA-256: | 0ED05F044B9A2D67FF494B4CA18BDA32521A50659540518BBE3C5E95B26E2118 |
| SHA-512: | 1EE9EC2B898182D748DDE18220CC2AD4391465B6F4F248A28ADDFBA57E46BDE0B501D74848648BA366CB046119A301633CB5CCC81B59A48C0DAC1ECFC11F6AC |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=7bff626b9d0443b99bd0c83ccec04554.IDENTIFIER=org.gnome.Shell.desktop. |

| /run/systemd/journal/streams/.#9:771952yGkh2 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 188 |
| Entropy (8bit): | 5.301611554202912 |
| Encrypted: | false |
| SSDEEP: | 3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm8rnTAAjAxsjshQJWQ:SbFuFyLVlg1BG+f+M8r8AsqjtWL0 |
| MD5: | E5C7CE42EE982C989C417E6985905E44 |
| SHA1: | 40F1BA242DAC2559DBD3DA07037F826A8E5B98CA |
| SHA-256: | DE35E9EE1ED3F3AC2FDFC4A54482066868F746C36F4030A73A2FD42379CC8464 |
| SHA-512: | 2A692D5801DE770DD9D466F48BE874CAC04DC0F293F35282E6E6B011D33DA7C67A297BA29514BDDA0B3A99DC0B08E154E8216E4D9651CB76787A2A8ADFBC79 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=62a4558d112a4831918e12ce61e42dda.IDENTIFIER=pulseaudio. |

| /run/systemd/journal/streams/.#9:77204UOi9C1 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 206 |
| Entropy (8bit): | 5.39346271966411 |
| Encrypted: | false |
| SSDEEP: | 3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxm4fBd0HG3Zes22js2O:SbFuFyLVlg1BG+f+M4/zZjNALQru+u |

| /run/systemd/journal/streams/.#9:77204UOi9C1 | |
|---|---|
| MD5: | 46291E51F3487941278E764036E17FA9 |
| SHA1: | 70A76DE12725BEF158832D9EF7925438ACF3E8D0 |
| SHA-256: | AFE4FDDD137A1604791D6B8B6F9A7FF4402DCEDE3F15F01F4C714A26BB21B35A |
| SHA-512: | 15145BAB207EB998B7D36B91730E86D726FBB78DF64673B1A4AE0D5650B629B6F492AB60405EE3046C73EBECDF4492178E3FCCA4D6714ACCD10CE47AD92608<br>4 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_<br>ID=288d633625ea4cecb81238840e63ab99.IDENTIFIER=geoclue.UNIT=geoclue.service. |

| /run/systemd/journal/streams/.#9:77270CWDpE0 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 217 |
| Entropy (8bit): | 5.42188471314324 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVK6g7/+BG+f+Mumq+lh0jFmShmWc0vn:qgFqo6g7/+0+f+Mm+lh+9kWc0vn |
| MD5: | F35762DD053AEAF841D321DC2DB52FEB |
| SHA1: | BFB205D23F0CDDCBE8BF59F5C3F32F47B0D79FA3 |
| SHA-256: | 1AD267A2292F65C9675AA5C597D2A96639F6E7C41A5667C11380EA24B1F066E9 |
| SHA-512: | B7219B2B125DB998AB128B5E9FB98EBA1F0BA7F7010DE2639BB139B10E5B33949E53E803128D2FF08186A9E6F5D7AA3B2C4980553B2536A39B017E0B74375EA0 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I<br>D=d3f2fb857d4e467da61f00115121722b.IDENTIFIER=org.gnome.SettingsDaemon.Sharing.desktop. |

| /run/systemd/journal/streams/.#9:77271Sl23z1 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 217 |
| Entropy (8bit): | 5.429376201186743 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVI6g7/+BG+f+M6z3d8H0jFmShmWc0vn:qgFqdg7/+0+f+MnH+9kWc0vn |
| MD5: | D3EBAAD4F5FE9F83D70849378C3C9825 |
| SHA1: | 4F3E386CD6BFB36393F328EDCF369119C173CA9A |
| SHA-256: | FA8DEC8D9E594F0556287E80A8A67FAF29A8DF3F4074F9CEE9AA51576505A560 |
| SHA-512: | 2A233E82209F859FB6416EFD6DB94D10FA94887F39C2680497B643F0D75B028F6469041B82FD46FEC97ED5B791E7289934908BF98ED9CEDE1A9CCD9BCB45B0E |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I<br>D=5c0451fd62e4412f89ce8a39007a87f2.IDENTIFIER=org.gnome.SettingsDaemon.Sharing.desktop. |

| /run/systemd/journal/streams/.#9:7727380DgqY | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 215 |
| Entropy (8bit): | 5.4301068576388305 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVK6g7/+BG+f+MHhuca0jFmShmVxfvn:qgFqo6g7/+0+f+M1a+9kVxfvn |
| MD5: | 04247A24669649B5DBCFC9B0694F9658 |
| SHA1: | 9B6675782439C53D4C5C8385A98EC798C3C744C5 |
| SHA-256: | 23895292D1D3BA98234187D998BE7E5F5D6F5C2611464D3B4AF798BB08FF4B52 |
| SHA-512: | ECC5B9093FC66CD568C5AAFAD36B6A01ECE01E9E9D58C947869CCDD3F4716445825128CDE9D1DFCFC87E038DE6638AA6959BC37A06E8432161261888CF854F<br>C |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I<br>D=c103dd82910f4b0487d8f9c148f96e9f.IDENTIFIER=org.gnome.SettingsDaemon.Wacom.desktop. |

| /run/systemd/journal/streams/.#9:77274Qs48r0 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 215 |

| /run/systemd/journal/streams/.#9:77274Qs48r0 | |
|---|---|
| Entropy (8bit): | 5.4464441551596945 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVI6g7/+BG+f+M+/g4RPjFmShmVxfvn:qgFqdg7/+0+f+MB4j9kVxfvn |
| MD5: | A38922143A3CC09DE8DA259D6693DCB3 |
| SHA1: | 656E7151880E9C4BA91CC4B3712D390198960067 |
| SHA-256: | 3944F2DED307840F6AF6E49C3E29014D20305FCC677EC71F8AE1E706E9D5F51E |
| SHA-512: | 3DB50B42A7C42DBFDA15347A18C612BB099BC750F3B64ADAE05EB5E878FE7A04D41E8B4A9D49AF39DDF911E0C213A03F8F7874E6033A4AFCF9D0D361D749FF<br>BF |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I<br>D=4abd5f0c825a4188b9aeb9f44777c263.IDENTIFIER=org.gnome.SettingsDaemon.Wacom.desktop. |

| /run/systemd/journal/streams/.#9:77296PViaL1 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 215 |
| Entropy (8bit): | 5.436361801307541 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVK6g7/+BG+f+M4Q4K9kZjFmShmDxfvn:qgFqo6g7/+0+f+M4xK9kv9kDBvn |
| MD5: | 0D031D6A8AD939B1698DC229D73AD8B9 |
| SHA1: | EACA54D791571693031829D5AA37CCA010B51C74 |
| SHA-256: | 345A7878DBBAD1F016060A2A811435E9BA45B79F563256F9BAEDA87CCFA3DB71 |
| SHA-512: | 13AC321A0F89F4ED529A3EC0AA12FCC6944C4E2FC11DF2B03F93E382F076FBB4075FDF4EF11B23BBF1223F9D591332E168F3C7435CF3A783F198538805180883 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I<br>D=26975a6cf2ff4c2fb4be1e3d922fc0c2.IDENTIFIER=org.gnome.SettingsDaemon.Color.desktop. |

| /run/systemd/journal/streams/.#9:77298iRbvl0 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 215 |
| Entropy (8bit): | 5.426280215265498 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVI6g7/+BG+f+M8zBJKqjFmShmDxfvn:qgFqdg7/+0+f+M8e49kDBvn |
| MD5: | 49B80CBDE8D4CF7EB4FC8D54C9442C6F |
| SHA1: | B673C00F02F248B07344483A0A3A2CB165B8B2AE |
| SHA-256: | FF04F32AC488FFF12828C84600F2C6A3D393A6FA5FE3DCF61FBFBC4A21F22ADD |
| SHA-512: | 60AAD7A439D2852EC2CA5F9FE7E9033AA643725E4B233A427784170F757C4A87DAFC4018AE3B4AC099C19DD8CB56D770B3B8A2800F55F93D72872D3D1EFF2BA<br>E |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I<br>D=6e0c6b0ad76a4a9b97002189f4c41367.IDENTIFIER=org.gnome.SettingsDaemon.Color.desktop. |

| /run/systemd/journal/streams/.#9:773003HAGfZ | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 218 |
| Entropy (8bit): | 5.396158949586181 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVK6g7/+BG+f+ME/Y9gUHgrqjFmShmxBrvn:qgFqo6g7/+0+f+ME/Y19kxBvn |
| MD5: | F76696F35C20C640C300EAB8375568A3 |
| SHA1: | D6113CF707F51BF379BCA8EC911E88DD58FFDEFF |
| SHA-256: | 336A05AF504F27D3AA7C423CA7FF4EF3B812F0AA920257C45E18D8CB90E3EF78 |
| SHA-512: | 6419BD9C3B6DCC4A8D31509DD60DA635AAD704A9D70A0D479B9A20AFC191859BE007C6AD7123B88BE9F5734ABB5D3CAD7F790539F7260A5BF0511F2A266699<br>4 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I<br>D=ed7e7bc966484de496330670b4c1b6da.IDENTIFIER=org.gnome.SettingsDaemon.Keyboard.desktop. |

| /run/systemd/journal/streams/.#9:77301hXDwj2 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |

| /run/systemd/journal/streams/.#9:77301hXDwj2 | |
|---|---|
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 218 |
| Entropy (8bit): | 5.4689768531684155 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVI6g7/+BG+f+MJB+2TU4jFmShmxBrvn:qgFqdg7/+0+f+MJuy9kxBvn |
| MD5: | 586C6FDBE63E0FA7115D2AD7CF5C5E2B |
| SHA1: | 9A45CC795546FB7DC0A12471FA17187C890D34B6 |
| SHA-256: | 3C4AC179C52E52BF5D65C8578EC13AB1652786C4917C0D024127B181E272AFB9 |
| SHA-512: | F3A3CA2D10013D110B79878ABF74BCE1431BC76181B065796F705953705C6F3460A72CEEF23D7403C03D66A11A3195E01C49E43104A60C563AF3D31570E19186 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=e8f9df92d93443dabb6cc58144b9871f.IDENTIFIER=org.gnome.SettingsDaemon.Keyboard.desktop. |

| /run/systemd/journal/streams/.#9:77324i5qr91 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 228 |
| Entropy (8bit): | 5.412081073610705 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVK6g7/+BG+f+M6fU8eg2jFmShm5PKJ0vn:qgFqo6g7/+0+f+M8U8fE9kYJ0vn |
| MD5: | 2C3DEC5EFE719F72E46807781AA39561 |
| SHA1: | 856F51FE95AF080A5C3A2D2727A81B7C8AA230ED |
| SHA-256: | 70ED85CD64425A86B63CFD3B4B2FD27B08C46029D03C3E417F9D6EE206639F9A |
| SHA-512: | F80E4753A4AA983A2259332A439A9A8F01CAFF4A6A49AAF8786048C6A4F3B713CB3C81BD7F0FAFC34C22F4B2B1C0000DDCA55420FF3447742C3CAD0FC926EF |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=0a5d12747495446f8ff841eda190346a.IDENTIFIER=org.gnome.SettingsDaemon.PrintNotifications.desktop. |

| /run/systemd/journal/streams/.#9:77326bi5ji2 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 228 |
| Entropy (8bit): | 5.424265174875916 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVI6g7/+BG+f+MsKCtdPAMiZjFmShm5PKJ0vn:qgFqdg7/+0+f+MsZdsv9kYJ0vn |
| MD5: | 997FF92F6A1D62586937DFF6A9FECCA2 |
| SHA1: | 47E74380329800605A16E66AA811E6281EF5BC5B |
| SHA-256: | 8131C87E365C69EC5E759DFC8F66ECF1465C9FC411E0B9AEB3EF69C03A9D2A13 |
| SHA-512: | 42173C48503C929F4E919BCEE2A2D6F2C830F50E6F3D2A338A87322754BFA0A3ECE315DE88279F46138CFDF95C3606DA76373AECC383AECEFECA61F3F5AEA6E0 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=e54c852d75734890bd383a0642e0fcb4.IDENTIFIER=org.gnome.SettingsDaemon.PrintNotifications.desktop. |

| /run/systemd/journal/streams/.#9:77348ac7ff1 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 216 |
| Entropy (8bit): | 5.439029997739953 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVK6g7/+BG+f+MSE9YOjFmShmatvn:qgFqo6g7/+0+f+MSC9katvn |
| MD5: | CE29B788CC84AB65E94A86450EAEE737 |
| SHA1: | 9DFC2B6BC2584F2D2FCDAED6B8C885E3F0A956E9 |
| SHA-256: | 6FFAC95A3C35295ECC0613ECD0690C09741FE012E839E6D56D243D969099ADAA |
| SHA-512: | 4A0C6CBE2CAF15CDE7DDE5DA216B0AE8A5EA33E409165AB55DC7AE0FEEDEC8717B42C4CBC08A9471A264EBB35243A9526FA4478358C2BE8783CDE5122630EE01 |
| Malicious: | false |

| /run/systemd/journal/streams/.#9:77348ac7ff1 | |
|---|---|
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=714b094dc7bf43a5bfa28adf4e16fbaa.IDENTIFIER=org.gnome.SettingsDaemon.Rfkill.desktop. |

| /run/systemd/journal/streams/.#9:77350tebHw0 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 216 |
| Entropy (8bit): | 5.4659252357707695 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVI6g7/+BG+f+M57klUMqjFmShmatvn:qgFqdg7/+0+f+M57AUM49katvn |
| MD5: | 51249612B105C63E2FA35ABCC9805EE4 |
| SHA1: | 0E14C2066C3F1CDCADEE646DE1192FBDFBAC0896 |
| SHA-256: | D3D572221FFA11A98BCCE4B7697175434943EF8F5FA1328245B8CBDC66D88EB4 |
| SHA-512: | DEC95540C99C71883C86B8ADBFC9DF78CA70734D509632320E47BED65A710401FA8302F0C5F56EA5E36AC57688FE0841B093B323AF7807FD5650D31DC0A3A1A |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=98e293cc36f445a6b0c9417a63889d3e.IDENTIFIER=org.gnome.SettingsDaemon.Rfkill.desktop. |

| /run/systemd/journal/streams/.#9:77352o84S8X | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 219 |
| Entropy (8bit): | 5.4480758827604605 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVK6g7/+BG+f+MoGQfQAqjFmShmzxvvn:qgFqo6g7/+0+f+MoGEX49kztvn |
| MD5: | E3FE64AD45E2555CB5F506B13C7576C7 |
| SHA1: | 35884387FE908CF1C7E3B963824F7C91E8FA4335 |
| SHA-256: | DD275C51873655F405A439BBDC5BC56254D983BE442C6F8F06CF7E89D4CFE9FD |
| SHA-512: | 92BBD9E262490BECD8D46DE74EF3AA9BF9E4230BBA87CFF2D0E84AAAEB9851382CDD821799135B2AE6A3F284A56CDC5157F49E804FF93057BFB774B7DF253725 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=b3d156785e174f5384afb287050c069a.IDENTIFIER=org.gnome.SettingsDaemon.Smartcard.desktop. |

| /run/systemd/journal/streams/.#9:77353lvB8VZ | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 219 |
| Entropy (8bit): | 5.4514489877467005 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVI6g7/+BG+f+MSYmyEjFmShmzxvvn:qgFqdg7/+0+f+MNlO9kztvn |
| MD5: | A9100D19FB72B37D17390E5B903B75D3 |
| SHA1: | 53450A9E3D5D893EC51B15A69B91C4B6F3D0915E |
| SHA-256: | 1EED3DF62354889F084BAE99CCEDCBC63E0BDE355121A9F17B07C5B9915A021D |
| SHA-512: | E7AA5B13CB31E944764CF40CAC7B16E00F9D72C34E942FFC463DCC901D63ECE15ED91826C20774EC1D7F89B50B3134AFCFC3BCB19AA8C0DB8A72B5ED19A3SB17 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=9748a6156b0747fb8b766f99613c399c.IDENTIFIER=org.gnome.SettingsDaemon.Smartcard.desktop. |

| /run/systemd/journal/streams/.#9:77355DbY2wY | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 218 |
| Entropy (8bit): | 5.402818369376012 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVK6g7/+BG+f+M9RX6jFmShmZBvn:qgFqo6g7/+0+f+M9RXI9kZBvn |
| MD5: | 23F4A768DFC5D58247CF2BF9FFC4D8CA |
| SHA1: | 185D2A135F8EF4B3D3B1B258E8BFE3DEA7A248DD |

| /run/systemd/journal/streams/.#9:77355DbY2wY | |
|---|---|
| SHA-256: | 5E27238B0F12AC543952F8782E36B8C890435F30C953D74F5A18A72B71A605F4 |
| SHA-512: | 0A6EA53B21001EAA66027FB87896E5690E85F93C4C3B7E37C865E00C759FDF4FB8EDF66D283FF7D7C32C15DF3CEC63114A720A9E1C619A43E40BC729E60E59F3 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=10414c415d8447c988b38da50b79d068.IDENTIFIER=org.gnome.SettingsDaemon.Datetime.desktop. |

| /run/systemd/journal/streams/.#9:77356FtwWiZ | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 218 |
| Entropy (8bit): | 5.410672726748514 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVI6g7/+BG+f+MTTokJ+72jFmShmZBvn:qgFqdg7/+0+f+MTTVL9kZBvn |
| MD5: | 7A32FDA62BAECB4FFE41065A728B6A06 |
| SHA1: | 185805154B6AC70CF25D97524AD45CDEC3CA9D37 |
| SHA-256: | C543F2C058D93E2AF9C9A123F553B0287E3130B19309F5B2FEC75B94735C25E6 |
| SHA-512: | 885D1D2FAE5C2283F80034E60A4EFB18E0C8879C2AD48D5D975B2CDE66570FD3C8C6291E2F00F4C8ABDB6980138570E39822967CCF90E1B48EA611DF616FC3( |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=32fd6ca58f2c4355b38736f285d65d4e.IDENTIFIER=org.gnome.SettingsDaemon.Datetime.desktop. |

| /run/systemd/journal/streams/.#9:773787pAHZZ | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 219 |
| Entropy (8bit): | 5.3770088147763975 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVK6g7/+BG+f+Mym7SUV1o7SAuqjFmShmwtvn:qgFqo6g7/+0+f+MtWUV4N9kwtvn |
| MD5: | E5365A5C530FCE147B1A39B2A9B61119 |
| SHA1: | 765C687BBEE06B0B9EF5514347F14EC0C676976B |
| SHA-256: | A1FF0E91C849789945BF0290A4C17213932ADFD400F5DDBD5F7BF7BB14A4A18B |
| SHA-512: | E6D9F32D10C0F866B792C89E0E4A74269C0E06E074B31A8E0FD821A2BB2C70729ADFBFDB8328C3F65E40471D9550C8E89DF1AA71297D0464F106B449DD2142B |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=8b8a8247107c4b4ebbdd04eb014e7a97.IDENTIFIER=org.gnome.SettingsDaemon.MediaKeys.desktop. |

| /run/systemd/journal/streams/.#9:77380wirAq1 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 219 |
| Entropy (8bit): | 5.411822916430001 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVI6g7/+BG+f+M4BfdMSXz4g2jFmShmwtvn:qgFqdg7/+0+f+M4BlTXze9kwtvn |
| MD5: | D32F9F6EE88597C49F51C70D28785CEE |
| SHA1: | A6B21B76D9B5ADE53845EED727AFA3E19C8E12B9 |
| SHA-256: | 568DF3A8EE5BE56055484E3BFFF4B04C40D97A2DB86054F4A04A9219F6C8F3E4 |
| SHA-512: | F442AEC575BEFA228880C56A070B6E4450A9682412721D3B194149FB2878B08601084D430DE1A6A0DC4D078101E15DAADA85DC4B9941DFB43D196DA1D4086EF |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=2df6823908ad4148aae7e649570d680b.IDENTIFIER=org.gnome.SettingsDaemon.MediaKeys.desktop. |

| /run/systemd/journal/streams/.#9:77402FeAcdZ | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 226 |
| Entropy (8bit): | 5.457982416867642 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVK6g7/+BG+f+M444ETjFmShmkiEovn:qgFqo6g7/+0+f+M444y9kVEovn |

| /run/systemd/journal/streams/.#9:77402FeAcdZ | |
|---|---|
| MD5: | AD17E69F2085458CFF23BB8F70E8E077 |
| SHA1: | F8A1E495582D8A8C25EA75BC912650E8164B2430 |
| SHA-256: | F910F4892D3B7E72164F93833261449B9A3AC84F4C8F91B79CDAF967D6ABB0AB |
| SHA-512: | 50CF2F3FF239D8DBB17E56A006BA250AAEBD556CE78663B69B5B4698224F2D14500C3874F00C28B8D79031FDCC91296CDF83B65BD29F6D02F56F45848EBD3A0B |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=29db3a4283cc49fba37401842982e830.IDENTIFIER=org.gnome.SettingsDaemon.ScreensaverProxy.desktop. |

| /run/systemd/journal/streams/.#9:77404dUif9Y | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 226 |
| Entropy (8bit): | 5.428611685400944 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVl6g7/+BG+f+M5QOMwRcrqjFmShmkiEovn:qgFqdg7/+0+f+Mpxcr49kVEovn |
| MD5: | C2041EC499688CC56F8CB479812E33AF |
| SHA1: | 4951C2D336059FC95F2A5622F5A74A0085E66DB8 |
| SHA-256: | 2D9033689340A28C871D700B66BA55F373DD1CF4ACBC449201224B9F1FEB430E |
| SHA-512: | D3F232394402EBE90DCA5E39DA98918F7ADE7C2D34B4B4BB4478443499FB2E3ABB4CF2E36D373FD5562DC5AF8B956EEDB371043B9B4BF257ACA718BDDE73A11 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=c76f99eaed8844f89c17f5c1ebef8c47.IDENTIFIER=org.gnome.SettingsDaemon.ScreensaverProxy.desktop. |

| /run/systemd/journal/streams/.#9:77427zUGoC1 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 215 |
| Entropy (8bit): | 5.443504925179464 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVK6g7/+BG+f+MbXZcjjJsZjFmShmpvn:qgFqo6g7/+0+f+M1U29kpvn |
| MD5: | CBF5ADD55EC36BD0A02E84F9CCD79BF5 |
| SHA1: | B19F89625E2C34130ECB11E72E1891EF40B27203 |
| SHA-256: | D4E49B12D3E8A366A8903A8BFC9FD3976A0B7CFB04250380702D7AA3A2ECD976 |
| SHA-512: | 7CD95DF814FCEC5CCAF1B5102ED710589B02C7516BFE61CC98B6A15C68DD67878756ACA71FD4D45BCE27F6663D107CF779B46BE1A52CF60F9F9232F2D2B3B8 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=921cd6e3674a497ab8e8ccd975759fe8.IDENTIFIER=org.gnome.SettingsDaemon.Sound.desktop. |

| /run/systemd/journal/streams/.#9:77429w9DKJ1 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 215 |
| Entropy (8bit): | 5.384179867029866 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVl6g7/+BG+f+M/hRnyTpjFmShmpvn:qgFqdg7/+0+f+M/hS9kpvn |
| MD5: | 04DA90480216ECBE0BF437148BF2737B |
| SHA1: | 6220DB50E83844BCEF8878713C55D1E46885B9B6 |
| SHA-256: | 0121FBC87449CA5E2BD6E97BABD1EA100B28448C5E3D0645F7868E3A0E389639 |
| SHA-512: | 4A97B4942C3FAF469C22847B7C8EE1AF32F8EEFD9768C26B48BDAB051584E35F98EDEE66BFFAD16B78869165F3C22FE327EB28AEF7191C53A72B79E9DE2FD1A |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=cd07dde895464ec8acf7884cac03396e.IDENTIFIER=org.gnome.SettingsDaemon.Sound.desktop. |

| /run/systemd/journal/streams/.#9:774316zlQSY | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |

| /run/systemd/journal/streams/.#9:774316zlQSY | |
|---|---|
| Size (bytes): | 222 |
| Entropy (8bit): | 5.423242928987812 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVK6g7/+BG+f+M6jFmShmQmc0vn:qgFqo6g7/+0+f+Ml9kQmtvn |
| MD5: | 437733DA30B895A2BD141CC39F3EBBFF |
| SHA1: | A5A1043C64CFD620CB7E42C96AFA16989A7F24E7 |
| SHA-256: | 1987AC3924CF6CBF73D44FA863C32E4713A0109A93A539BEE0A461B203A1EE88 |
| SHA-512: | 462BC191D8107CD8DADCFDA5E0F6BE6C2CFAF9C7A35A10924472BB836D86F88B9BB009354587FACEE5308066F83761672683EBEC69094A2D70666C12DCF1E2<br>9 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I<br>D=794e27b858e944e7ba019c0cf72a284e.IDENTIFIER=org.gnome.SettingsDaemon.A11ySettings.desktop. |

| /run/systemd/journal/streams/.#9:77432qJDZbY | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 222 |
| Entropy (8bit): | 5.381695385591385 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVI6g7/+BG+f+M6ppa7df0jFmShmQmc0vn:qgFqdg7/+0+f+MKYg9kQmtvn |
| MD5: | 9DC1C47D26CB93DC3FDAC47D6311112C |
| SHA1: | 2846553EB6FBCED58346CB365E3CEEFA9CEB994E |
| SHA-256: | 7C685487C115A0FD63EAEE0CDA549F4D6BE8F282DF740B987EDB6834B6BC990C |
| SHA-512: | 5CF1AB28622E67BBE48A576A82B65E43A902371D7560C197750FFE803AF732D4CEBBCBB11992FA819B3A5F8699BFD107885A9F4A71D415B52A1157943C232A01 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I<br>D=0a536a208ced45f48ae05b3cea3a0366.IDENTIFIER=org.gnome.SettingsDaemon.A11ySettings.desktop. |

| /run/systemd/journal/streams/.#9:77456l49Zr1 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 222 |
| Entropy (8bit): | 5.486110615012854 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVK6g7/+BG+f+M6Iu8jFmShmx+0vn:qgFqo6g7/+0+f+Mtu29k40vn |
| MD5: | 57DB98346179723183DD5447D2ED83B8 |
| SHA1: | E3DB5F18A6E7467574E2A5FD3A2A4B0B86DF2BE9 |
| SHA-256: | C84A3F62B7F070F12C865AB937397C6C5BC1172355A7F76967E7CB9EE4305F07 |
| SHA-512: | D22B39586EA460E4CCBABDED4122939D8AB600BDC9341358F6B42536D44553D313367E4FE062D48EF4037ED3D722F248BDD97D79C9D2D45C27DFCD81AFB845<br>F |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I<br>D=08296a491dfd4b38838b55787b6c74bd.IDENTIFIER=org.gnome.SettingsDaemon.Housekeeping.desktop. |

| /run/systemd/journal/streams/.#9:77457MUtD7Y | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 222 |
| Entropy (8bit): | 5.46060924756978 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVI6g7/+BG+f+McS4Ja40jFmShmx+0vn:qgFqdg7/+0+f+Mae9k40vn |
| MD5: | F3E99D803CAE6EF2164065E187C1E75C |
| SHA1: | 5E1C3BCF3B11AEC2BFEF4B5E1BEF0C7314FA2F9E |
| SHA-256: | 456BB97FE2C50F227810CE13651FC76440C98B501DEAA2F90AB643097FB2FE2F |
| SHA-512: | 1BC7985FC729F803045F898B89F370F09CAB6B4BB54552D3754868D105B0B6C23C495347ED75067B973D5E92F0BCE3B54CFC744E0A97C8AB7C90B3993431AED |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I<br>D=3ef3007bae4f4c8c9682b5e902609c15.IDENTIFIER=org.gnome.SettingsDaemon.Housekeeping.desktop. |

| /run/systemd/journal/streams/.#9:774810NRVf2 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 215 |
| Entropy (8bit): | 5.430031613405449 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVK6g7/+BG+f+MszBdCD602jFmShm3vn:qgFqo6g7/+0+f+MszLCDbE9k3vn |
| MD5: | 86724200BB8186C18D89DD9A8EFB581E |
| SHA1: | 465A99DFB44F10B215B12B2A3B96075C17DB62CE |
| SHA-256: | 41D99B3BD91E60ECABF171E6F23338590B6DE02E29A2047CF4A20EA2C9957EAC |
| SHA-512: | C2F2FE18E08AC625B7CDE8EDAB5E589E89E0DEC0ED0F84816446B9A0AE3B3DF823B3D919095C1DA8B746CD8E98F247D9B355DD01AB61F453B9627DE71EAF7D39 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=f8b37dc8de9e431193f13794d188fe46.IDENTIFIER=org.gnome.SettingsDaemon.Power.desktop. |

| /run/systemd/journal/streams/.#9:774830x5zg2 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 215 |
| Entropy (8bit): | 5.40123799207827 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVI6g7/+BG+f+MFVETjFmShm3vn:qgFqdg7/+0+f+MFVEN9k3vn |
| MD5: | 5335999FBED68186C87B29FD4CBD33AE |
| SHA1: | 690940AEECF02E15BA7349397FB77523ADCC7F89 |
| SHA-256: | B8571C94328128DDA369DCA61718583A80534B5B82EDE66B3FF9D266B4DCFDA7 |
| SHA-512: | 6A09C4C7EB71C125781BDCAFD57693BD2CCA237B5E57EEF0308F3EB86ACC2EF22F6EB09D0F18AC4BADB579242C4B9AAD123767ECEB157538E468523F19556F7A |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=add43fa656bc4e978158e50ebb8e8e3a.IDENTIFIER=org.gnome.SettingsDaemon.Power.desktop. |

| /run/systemd/journal/streams/.#9:77680l5uWQ1 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 226 |
| Entropy (8bit): | 5.460932431338503 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVIg1BG+f+M8EeQXw3xEN2jZcHdzqDq:qgFq6g10+f+M87x3mQDq |
| MD5: | 1C7DEF7329A50576DF0953649BBB9F20 |
| SHA1: | 839D4392C250A6C08D3AE9E24BD56104A5E93AD4 |
| SHA-256: | 22BC41C47EE3EF4423B5FFE7FA7F7B88BA97AA003D84C8BC2F5D7E44380FE627 |
| SHA-512: | 23F8F925671DE00F1299D289BA2B007767953D5E98457256EC0362694C7358F72DD778FEF36BECC4C871574909EB0668A694B9ABA8C6AA63053DECE888579F69 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=64da0db75fc943b2849ab085cfb7a9f6.IDENTIFIER=systemd-hostnamed.UNIT=systemd-hostnamed.service. |

| /run/systemd/journal/streams/.#9:78349klwL2Z | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 206 |
| Entropy (8bit): | 5.36556698541765 |
| Encrypted: | false |
| SSDEEP: | 3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmrIMFwxGSN2lsjs3M+:SbFuFyLVIg1BG+f+MU782jXjK |
| MD5: | 2FEBFA1A4C2A09C25E60BD28BBBEF6EE |
| SHA1: | 54BAE3D790ED639E37D08BD40943263E60506086 |
| SHA-256: | B7F0CA6BDBE23AF21CDD9F370090F7E80A642F9416FEBC6A0825DC74FD41CB65 |
| SHA-512: | 7A128B75BB008AF52396E2B86F8EDF5A77C444EA7849523C85C3EC454A400624B146E63C577D0FAD80466BC785ED1A4FA3BC9BB34F259F1980DA6D908E7C795 |
| Malicious: | false |

| /run/systemd/journal/streams/.#9:78349klwL2Z | |
|---|---|
| Preview: | # This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=aafdc64ff00a4b85a942f2bd3dbc74b1.IDENTIFIER=fprintd.UNIT=fprintd.service. |

| /run/systemd/journal/streams/.#9:78521clZnq1 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 222 |
| Entropy (8bit): | 5.4034589004868625 |
| Encrypted: | false |
| SSDEEP: | 3:SbFVVmFyinKMsPOYsn9ms954Hh6SnLAqC+h6KV+h6CQzuxmr+qQoTTnRpv8jsicT:SbFuFyLVIg1BG+f+MirofnRijZcH5CHq |
| MD5: | FB90ACDD62415E682396486C38B1628D |
| SHA1: | 0AB1EB59EF6AF8998FFC7DB62E1BC4CF5A881466 |
| SHA-256: | 8118FD11E2DFCE8772A42B683786880A8FE6743001BB3EAFE39BA360324D8BA1 |
| SHA-512: | 5FB2C6029809391DDF5BBA8B5494F37FDBE11316949B148A1990038FB2373679515DD40E3A15944D60FFCC758C35A830398094839155A60069B81EC85AF8253B |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=a0117a0c36814385ad66ea42f3c0418e.IDENTIFIER=systemd-localed.UNIT=systemd-localed.service. |

| /run/systemd/journal/streams/.#9:78866O4Nfq2 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 228 |
| Entropy (8bit): | 5.466454339060342 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVIg1BG+f+MLEWjFZjdCt/rRMtq:qgFq6g10+f+MwWjxCDL |
| MD5: | F38C343B2FC2D43A1DC4449C6C495B93 |
| SHA1: | 9F41515204C08AD4328D072C353AD532DE2B3FAE |
| SHA-256: | 4058A11CACEFC44B43452686D73F0BA5B2360367AA3B4A8F91207A18A3C3293D |
| SHA-512: | 5218688F8067966132F5264A72621869A5413825E77599815CEB87E6A1EE52EFAFA6D86D1E35B8D3E50D0D1A5E3266A7FA30A662DF354F416E08BF62EE69ED0E |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=30.LEVEL_PREFIX=1.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=e8857df3299c465aa3613b5035d74ed8.IDENTIFIER=whoopsie-upload-all.UNIT=apport-autoreport.service. |

| /run/systemd/journal/streams/.#9:79191wy1PfZ | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 198 |
| Entropy (8bit): | 5.367018153940666 |
| Encrypted: | false |
| SSDEEP: | 6:SbFuFyLVK6g7/+BG+f+M4JG26wQHQjZarvn:qgFqo6g7/+0+f+M4IdGarvn |
| MD5: | 4D0952F499B11C374758A05C818FD840 |
| SHA1: | 2F0DA9662C5403206F5E5DA8CE7240717547C373 |
| SHA-256: | 94C3A9CB3C1002DB934DFEEE50F977BC670BF3D80086B263824B44F62AE23058 |
| SHA-512: | 5546497B82828075D17E3EA454B431811A9AB228FA5A66679E6E0B4ED09CAACAA8D735BE3EE9CBC617F3B83BFFF254E9DA800CDDB6339E31D38FFA54F05AB990 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_ID=23a0cf42cd0648de9df5dce021a57d28.IDENTIFIER=spice-vdagent.desktop. |

| /run/systemd/journal/streams/.#9:791933Ci8T1 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 198 |
| Entropy (8bit): | 5.390249186792024 |
| Encrypted: | false |
| SSDEEP: | 3:SbFVVmFyinKMsPOfvP69ms947z+h6SnLAqC+h6KV+h6CQzuxmuzdY8Rdicc8RqjG:SbFuFyLVI6g7/+BG+f+MuzTj+jZarvn |
| MD5: | 802E74C374724B91D0E7909770CD5579 |
| SHA1: | 8E47BB7D0D1DB0A5B2F811F43C468F8393260DCE |
| SHA-256: | 24E5FAC9953EA959D1D157BC8BDA3FAD14E59B77BD6449012FBFEEA8898A25E4 |

| /run/systemd/journal/streams/.#9:791933Ci8T1 | |
|---|---|
| SHA-512: | 0D60FD0FD88E27C0119D3D637793C54349BFBBF4235A7C5237FCD50FC63AEA07A73390D268C69006ACA89BA1C383033C49A432FC9B82D1EC9BCBFC8EF7B1F3<br>5 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I<br>D=db79bdfefc8e447f961448912027997d.IDENTIFIER=spice-vdagent.desktop. |

| /run/systemd/journal/streams/.#9:79222vzLRU1 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 192 |
| Entropy (8bit): | 5.34992329020179 |
| Encrypted: | false |
| SSDEEP: | 3:SbFVVmFyinKMsPOdvP69ms947z+h6SnLAqC+h6KV+h6CQzuxm9oD31SHhTE90dI7:SbFuFyLVK6g7/+BG+f+MWDlSHtE92A22 |
| MD5: | 2B1DC7829848AB1FFEEA577A98130031 |
| SHA1: | 0123948048F720D58C25C10F6A5848F0E244F9A9 |
| SHA-256: | E9F83C9005C944203191E43CFFB44CFA67E457C3BF8CF895CB15074AC8215CC2 |
| SHA-512: | 2819849952683848C6B83B1C02F04D354066445C25DF8D22036AD10E5499DF34BF0ED292FD8AF4371CA63D0D0FDEB8120355B8E1D967C6A42A70A7C63C91C38 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=6.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I<br>D=71e3f9c0c17b4b56aae1a01ae3f81ab3.IDENTIFIER=xbrlapi.desktop. |

| /run/systemd/journal/streams/.#9:79224TSZ581 | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 192 |
| Entropy (8bit): | 5.340667136694104 |
| Encrypted: | false |
| SSDEEP: | 3:SbFVVmFyinKMsPOfvP69ms947z+h6SnLAqC+h6KV+h6CQzuxm92RfUXlDDU+vsjq:SbFuFyLVl6g7/+BG+f+MU8JKj022vn |
| MD5: | FF76DAC67534840163452F372D70387E |
| SHA1: | F9F5BA53FCDD3A1C9D9DEC630EC0D340D0A95AEF |
| SHA-256: | A6AC2EB76A5DE40688F0A653D6FDCAA616C963F0A321B2BBE4A89A0EE7FFE866 |
| SHA-512: | D9AA69ACD7F7F4A2A3E3156204380BD7B597A0F713A68D9949990791DCD4A1E44FF92403132EBA1A360A8B9362C89A72B08B7A1D73365A24F842C60422C98FC3 |
| Malicious: | false |
| Preview: | # This is private data. Do not parse.PRIORITY=4.LEVEL_PREFIX=0.FORWARD_TO_SYSLOG=0.FORWARD_TO_KMSG=0.FORWARD_TO_CONSOLE=0.STREAM_I<br>D=7d5d4529dab24ffb855d41ed4026ffaa.IDENTIFIER=xbrlapi.desktop. |

| /run/user/1000/pulse/pid | |
|---|---|
| Process: | /usr/bin/pulseaudio |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 5 |
| Entropy (8bit): | 2.321928094887362 |
| Encrypted: | false |
| SSDEEP: | 3:DdSv:Bc |
| MD5: | A3AE4AEA7302D578C3C3507088EB91BB |
| SHA1: | A199C6929741690546FC7C31F2F359372A872E02 |
| SHA-256: | 7EF143B2AB6278B57DE3A90232D7D430921A4133A085F2C2CFF3E49013BF738E |
| SHA-512: | C5D0FC5028A1485FD9E91E340C6020A2B42438FC54CE4B7DDBD0C741A0AA46B8DE39096DCE90D6D5FED68DF960905DF69F04150FE72E39682B24F9247DC6DE<br>4 |
| Malicious: | false |
| Preview: | 5387. |

| /run/user/127/ICEauthority | |
|---|---|
| Process: | /usr/libexec/gnome-session-binary |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 1304 |
| Entropy (8bit): | 5.9689611558550055 |
| Encrypted: | false |
| SSDEEP: | 12:OxPipveY+iaxPrKeveY+rK0h/7SxP5mhijveY+5tWmxPwWoveY+wcZVveY+wYvxG:0+9owqrbEn7 |
| MD5: | 6731B47EA3D1F57FE9650C0C73CF6060 |

| /run/user/127/ICEauthority | |
|---|---|
| SHA1: | E794B31257496E9F8A945F1C2ACB0DABA37A6200 |
| SHA-256: | F97E04D108935476B12A3892D877DD5236EA264E8BC4C801FCDFAE84824A545C |
| SHA-512: | AD6B6DDB2B1CCE9C7BC858B8958E34A238F9DA9E7EEBFA4834D15ABD7E199FB9E10A87941969DEFA74730B883B768DC5B6D7A1534564763AAB85FD2A8CCF97EC |
| Malicious: | false |
| Preview: | ..XSMP...!unix/galassia:/tmp/.ICE-unix/5531..MIT-MAGIC-COOKIE-1..H@I.f.8. a.R....XSMP...#local/galassia:@/tmp/.ICE-unix/5531..MIT-MAGIC-COOKIE-1..[n]...E.J...=.<br>e8..ICE...!unix/galassia:/tmp/.ICE-unix/5434..MIT-MAGIC-COOKIE-1....%QHV..pK-...V...ICE...#local/galassia:@/tmp/.ICE-unix/5434..MIT-MAGIC-COOKIE-1.....(es.v3..<br>..l$..XSMP...!unix/galassia:/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1...p.....A.9%..XSMP...#local/galassia:@/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1.....o.(R...}<br>.9...ICE...!unix/galassia:/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...w$....^.'fl..1..ICE...#local/galassia:@/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...^f.....E<br>..c..XSMP...#local/galassia:@/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1... .....Y...@.t...XSMP...!unix/galassia:/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...#...,.:B<br>.o.....ICE...#local/galassia:@/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1..N..yte\|4yXJ...Mf..ICE...!unix/galassia:/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1.....cN...<br>..N+..$..XSMP...#local/galass |

| /run/user/127/dconf/user | |
|---|---|
| Process: | /usr/libexec/gsd-power |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:: |
| MD5: | 93B885ADFE0DA089CDF634904FD59F71 |
| SHA1: | 5BA93C9DB0CFF93F52B521D7420E43F6EDA2784F |
| SHA-256: | 6E340B9CFFB37A989CA544E6BB780A2C78901D3FB33738768511A30617AFA01D |
| SHA-512: | B8244D028981D693AF7B456AF8EFA4CAD63D282E19FF14942C246E50D9351D22704A802A71C3580B6370DE4CEB293C324A8423342557D4E5C38438F0E36910EE |
| Malicious: | false |
| Preview: | . |

| /run/user/127/gdm/Xauthority | |
|---|---|
| Process: | /usr/lib/gdm3/gdm-x-session |
| File Type: | X11 Xauthority data |
| Category: | dropped |
| Size (bytes): | 104 |
| Entropy (8bit): | 4.983294787198872 |
| Encrypted: | false |
| SSDEEP: | 3:rg/WFllasO935/7KAo+a3tWFllasO935/7KAob:rg/WFl2hKAbOWFl2hKAM |
| MD5: | BFC768D4E3FE88DEFDD3D34B6EAA4D46 |
| SHA1: | DB2AD84EE50C218E60CD9BC54ED3345DD2756F8E |
| SHA-256: | AF151F85930E23739C4455D77972C12902CE1A2D4C2783B1B0A5BE57D4CB5B43 |
| SHA-512: | DEFA3084E8821B666FB704C3DFD0505F6EC8923994EF1B20FCCA536C1A12981899D453D2687797DE3C8340CB4249F00EF6B7D5C902CFCF3871E3BB1584167CC |
| Malicious: | false |
| Preview: | ....galassia....MIT-MAGIC-COOKIE-1....o.X.....\%.!.....galassia....MIT-MAGIC-COOKIE-1....o.X.....\%.!. |

| /run/user/127/pulse/pid | |
|---|---|
| Process: | /usr/bin/pulseaudio |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 5 |
| Entropy (8bit): | 2.321928094887362 |
| Encrypted: | false |
| SSDEEP: | 3:JVTv:bTv |
| MD5: | 9822AB275604B3E5C3DB54857133F1D1 |
| SHA1: | 50A34638C205A321B717BE868BD409F8D4BD684C |
| SHA-256: | 2CD5DAA9B4AEAC2047E3FA3F0BD5AA6FF46BE14DD6DDE971DBAE471099062CB2 |
| SHA-512: | 2997E41D5406726125DF1640B9385B9A8A7A947B667A1FDB9063C18C6BC946C75C37548665984E5CC037EC11D9875613BC62AD30988DCE6E3E7F9B77631AB756 |
| Malicious: | false |
| Preview: | 5906. |

| /tmp/server-0.xkm | |
|---|---|
| Process: | /usr/bin/xkbcomp |
| File Type: | Compiled XKB Keymap: lsb, version 15 |
| Category: | dropped |
| Size (bytes): | 12060 |
| Entropy (8bit): | 4.8492493153178975 |

| /tmp/server-0.xkm | |
|---|---|
| Encrypted: | false |
| SSDEEP: | 192:tDyb2zOmnECQmwTVFfLaSLus4UVcqLkjoqdD//HJeCQ1+JdDx0s2T:tDyAxvYhFf+S6tUzmp7/1MJ |
| MD5: | B4E3EB0B8B6B0FC1F46740C573E18D86 |
| SHA1: | 7D35426357695EBA77850757E8939A62DCEFF2D1 |
| SHA-256: | 7951135CC89A6E89493E3A9997C3D9054439459F8BFCE3DDEC76B943DA79FA91 |
| SHA-512: | 8196A23E2B5E525A5581562A2D7F2EE4FF5B694FEF3E218206D52EA9BFE80600BB0C6AA8968CA58E93E1AAD478FA05E157D08DB6D4D1224DDEA6754E377BE0<br>1 |
| Malicious: | false |
| Preview: | .mkx.....D.....h.....<.....P.@%.....&.....D.....NumLock.....Alt.....LevelThree..LAlt....RAlt....RControl....LControl....ScrollLock..LevelFive...AltGr...Meta<br>....Super...Hyper.....evdev+aliases(qwerty)...!.....ESC.AE01AE02AE03AE04AE05AE06AE07AE08AE09AE10AE11AE12BKSPTAB.AD01AD02AD03AD04AD05AD<br>06AD07AD08AD09AD10AD11AD12RTRNLCTLAC01AC02AC03AC04AC05AC06AC07AC08AC09AC10AC11TLDELFSHBKSLAB01AB02AB03AB04AB05AB06AB07AB<br>08AB09AB10RTSHKPMULALTSPCECAPSFK01FK02FK03FK04FK05FK06FK07FK08FK09FK10NMLKSCLKKP7.KP8.KP9.KPSUKP4.KP5.KP6.KPADKP1.KP2.KP<br>3.KP0.KPDLLVL3....LSGTFK11FK12AB11KATAHIRAHENKHKTGMUHEJPCMKPENRCTLKPDVPRSCRALTLNFDHOMEUP..PGUPLEFTRGHTEND.DOWN<br>PGDNINS.DELEI120MUTEVOL-VOL+POWRKPEQI126PAUSI128I129HNGLHJCVAE13LWINRWINCOMPSTOPAGAIPROPUNDOFRNTCOPYOPENPASTFI<br>NDCUT.HELPI147I148I149I150I151I152I153I154I155I156I157I158I159I160I161I162I163I164I165I166I167I168I169I170I171I172I173I174I175I176I177I178I179I180I181<br>I182I183I184I185I186I187I188I189I190FK13FK14FK15FK16FK17FK18 |

| /var/lib/AccountsService/users/gdm.W29KC1 | |
|---|---|
| Process: | /usr/lib/accountsservice/accounts-daemon |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 61 |
| Entropy (8bit): | 4.66214589518167 |
| Encrypted: | false |
| SSDEEP: | 3:urzMQvNT+PzKLrAan4R8AKn:gzMQIzKLrAa4M |
| MD5: | 542BA3FB41206AE43928AF1C5E61FEBC |
| SHA1: | F56F574DAF50D609526B36B5B54FDD59EA4D6A26 |
| SHA-256: | 730D9509D4EAA7266829A8F5A8CFEBA6BBDDD5873FC2BD580AD464F4A237E11A |
| SHA-512: | D774B8F191A5C65228D1B3CA1181701CFCD07A3D91C5571B0DDF32AD3E241C2D7BDFC0697AB97DC10441EF9CDC8AEE5B19BC34E13E5C8B0B91AD06EEF42F<br>AEA |
| Malicious: | false |
| Preview: | [User].XSession=.Icon=/var/lib/gdm3/.face.SystemAccount=true. |

| /var/lib/AccountsService/users/gdm.WIY8B1 | |
|---|---|
| Process: | /usr/lib/accountsservice/accounts-daemon |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 61 |
| Entropy (8bit): | 4.66214589518167 |
| Encrypted: | false |
| SSDEEP: | 3:urzMQvNT+PzKLrAan4R8AKn:gzMQIzKLrAa4M |
| MD5: | 542BA3FB41206AE43928AF1C5E61FEBC |
| SHA1: | F56F574DAF50D609526B36B5B54FDD59EA4D6A26 |
| SHA-256: | 730D9509D4EAA7266829A8F5A8CFEBA6BBDDD5873FC2BD580AD464F4A237E11A |
| SHA-512: | D774B8F191A5C65228D1B3CA1181701CFCD07A3D91C5571B0DDF32AD3E241C2D7BDFC0697AB97DC10441EF9CDC8AEE5B19BC34E13E5C8B0B91AD06EEF42F<br>AEA |
| Malicious: | false |
| Preview: | [User].XSession=.Icon=/var/lib/gdm3/.face.SystemAccount=true. |

| /var/lib/gdm3/.config/ibus/bus/ee49dfd4fa47433baee88884e2d7de7c-unix-0 | |
|---|---|
| Process: | /usr/bin/ibus-daemon |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 381 |
| Entropy (8bit): | 5.15610597737776 |
| Encrypted: | false |
| SSDEEP: | 6:SbF4b2sONeZVkSoQ65EfqFFAU+qmnQT23msRvkTFacecf8h/zKLGWWOT21NB/zmQ:q5sU3LWfLUDmQymqSFbfomSkT21NB/iQ |
| MD5: | 33EA15852DABAF1B37E3B2912671F64A |
| SHA1: | CE9B74C4500D92BFE468D2BA83F8515198F0E67B |
| SHA-256: | 33A8588CA6E7D6F9D8B8277BBAC03A45F44985EA5D6730FDCFD4E447352469E9 |
| SHA-512: | 9BCA9867D04298E00519F64210A155732EB61C426F8B05FBD604DC592D0DBE2FBBBBC634A652E77868AAE768B1C1B8BAB524EB97072994FF7CC217AA727248A<br>E |
| Malicious: | false |

| /var/lib/gdm3/.config/ibus/bus/ee49dfd4fa47433baee88884e2d7de7c-unix-0 | |
|---|---|
| Preview: | # This file is created by ibus-daemon, please do not modify it..# This file allows processes on the machine to find the.# ibus session bus with the below address..# If the IBUS_ADDRESS environment variable is set, it will.# be used rather than this file..IBUS_ADDRESS=unix:abstract=/var/lib/gdm3/.cache/ibus/dbus-AUvSPQIo,guid=fb2a1ad38261d5c79322114161807b33.IBUS_DAEMON_PID=5646. |

| /var/lib/gdm3/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-sink | |
|---|---|
| Process: | /usr/bin/pulseaudio |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:v:v |
| MD5: | 68B329DA9893E34099C7D8AD5CB9C940 |
| SHA1: | ADC83B19E793491B1C6EA0FD8B46CD9F32E592FC |
| SHA-256: | 01BA4719C80B6FE911B091A7C05124B64EEECE964E09C058EF8F9805DACA546B |
| SHA-512: | BE688838CA8686E5C90689BF2AB585CEF1137C999B48C70B92F67A5C34DC15697B5D11C982ED6D71BE1E1E7F7B4E0733884AA97C3F7A339A8ED03577CF74BE09 |
| Malicious: | false |
| Preview: | . |

| /var/lib/gdm3/.config/pulse/ee49dfd4fa47433baee88884e2d7de7c-default-source | |
|---|---|
| Process: | /usr/bin/pulseaudio |
| File Type: | very short file (no magic) |
| Category: | dropped |
| Size (bytes): | 1 |
| Entropy (8bit): | 0.0 |
| Encrypted: | false |
| SSDEEP: | 3:v:v |
| MD5: | 68B329DA9893E34099C7D8AD5CB9C940 |
| SHA1: | ADC83B19E793491B1C6EA0FD8B46CD9F32E592FC |
| SHA-256: | 01BA4719C80B6FE911B091A7C05124B64EEECE964E09C058EF8F9805DACA546B |
| SHA-512: | BE688838CA8686E5C90689BF2AB585CEF1137C999B48C70B92F67A5C34DC15697B5D11C982ED6D71BE1E1E7F7B4E0733884AA97C3F7A339A8ED03577CF74BE09 |
| Malicious: | false |
| Preview: | . |

| /var/log/Xorg.0.log | |
|---|---|
| Process: | /usr/lib/xorg/Xorg |
| File Type: | ASCII text |
| Category: | dropped |
| Size (bytes): | 41347 |
| Entropy (8bit): | 5.2780610136481165 |
| Encrypted: | false |
| SSDEEP: | 384:JvazrJ8u+NM7dadGd1dIdzdbdddSdndwd3dYdVdUdGdHdbdFdOd5dtBdHFdx9dN7:Ezrqu56s7j7GUtGD1Z8dC+c |
| MD5: | F2BFDB49C32E8B0F548F10BE463577F1 |
| SHA1: | 62C470D277D0B566E7438030A40E0F4D7A22791D |
| SHA-256: | B9067CA0C55A92C3A1973BC983D9DF0C30C8AFDD871138031CE373EB71A21E36 |
| SHA-512: | 9920580D0073817945ED001D9898E019217209898E0AAD6AAF6A03A9BA4D87075D136C5B4DD962A863622FFD10C908B97B3E4EB8C7CBDFC53F103541D129C859 |
| Malicious: | false |
| Preview: | [ 502.823] (--) Log file renamed from "/var/log/Xorg.pid-5486.log" to "/var/log/Xorg.0.log".[ 503.227] .X.Org X Server 1.20.11.X Protocol Version 11, Revision 0.[ 503.574] Build Operating System: linux Ubuntu.[ 503.623] Current Operating System: Linux galassia 5.4.0-72-generic #80-Ubuntu SMP Mon Apr 12 17:35:00 UTC 2021 x86_64.[ 503.635] Kernel command line: Patched by Joe: BOOT_IMAGE=/vmlinuz-5.4.0-72-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro maybe-ubiquity.[ 503.652] Build Date: 06 July 2021 10:17:51AM.[ 503.656] xorg-server 2:1.20.11-1ubuntu1~20.04.2 (For technical support please see http://www.ubuntu.com/support) .[ 503.660] Current version of pixman: 0.38.4.[ 503.664] .Before reporting problems, check http://wiki.x.org..to make sure that you have the latest version..[ 503.668] Markers: (--) probed, (**) from config file, (==) default setting,..(++) from command line, (!!) notice, (II) informational,..(WW) warning, (EE) error, (NI) not implemented, (??) |

| /var/log/journal/ee49dfd4fa47433baee88884e2d7de7c/system.journal | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 240 |
| Entropy (8bit): | 1.4428593527838254 |
| Encrypted: | false |
| SSDEEP: | 3:F31HliryTOyryTO:F3Yyzy |

| /var/log/journal/ee49dfd4fa47433baee88884e2d7de7c/system.journal | |
|---|---|
| MD5: | E442B3625BB6B4A1D945453A307F7033 |
| SHA1: | 4C4F7CEE460CF1E899E15FB180A9D2077FFCF824 |
| SHA-256: | 81B027BFF663FCDAB98746F999060A38FFDCC77848180BD7F17C3EC98A46F883 |
| SHA-512: | F23AFCCCFF5B59985349E9CA02444D4EF63EAC6F397B5499D54BA2B384A9C96B0F38F3011884BAF83BB4D28367CFF744F4C5F89F7DD1FDA81C69B794618AB08 |
| Malicious: | false |
| Preview: | LPKSHHRH.....i.N$..X..h,o.....i.N$..X..h,o..... |

| /var/log/journal/ee49dfd4fa47433baee88884e2d7de7c/user-1000.journal | |
|---|---|
| Process: | /lib/systemd/systemd-journald |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 240 |
| Entropy (8bit): | 1.4261926861171588 |
| Encrypted: | false |
| SSDEEP: | 3:F31HleGg3JYgGg3J4l:F3uxal |
| MD5: | 63CF349BF3D4379DC5CB3C2225243A8E |
| SHA1: | 08B3A4FEF2AD93AE6649965065CB35F40BB69D31 |
| SHA-256: | E0A8E816AA305A170402899F8E1D025DBB0B483B2BDDBAF156E24DC7C6AD8D3A |
| SHA-512: | E95ED5B442CAF68F36019F3AE41B0A13D90CAA4BB152B8F1B89624884D6C601951B429B64D864D8B53A64504966EE08C38567B5CBB12382023E716D8282F23E4 |
| Malicious: | false |
| Preview: | LPKSHHRH.....o....O.....l-.....o....O.....l-..... |

# Static File Info

## General

| | |
|---|---|
| File type: | ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped |
| Entropy (8bit): | 5.436290827716319 |
| TrID: | • ELF Executable and Linkable format (generic) (4004/1) 100.00% |
| File name: | 8PRjJeUifB |
| File size: | 100836 |
| MD5: | 0edbe8b6af0b271b496686bf87db10d7 |
| SHA1: | a22440162f3d3e651ff2673d9073966edffb16cd |
| SHA256: | 6d1237a9ce13466c91ad2c3558719afe931bc47a00e0b15b9558574f5f030e23 |
| SHA512: | 554c1793745d3ec028d0610eca2804b22941a6cd7ad851c29499d08c52510cce57ca2f0678dd18739d469249edb16ff8b326bf104b38a2313751c394f62a5033 |
| SSDEEP: | 1536:YJg/zEgGtTStvjE5S80VOYzHJxotsU1NtWMbrKaleHukA:K2zEHS+mOqpxotsU1+MbrKankA |
| File Content Preview: | .ELF.....@.`...4.....4. ...(.....@...@....u...u.....E...E.....P..+.....dt.Q.....<..'..\|...l'.....<...'..X...!... ....'9... .....<...'..(...!.....'9\ |

## Static ELF Info

| ELF header | |
|---|---|
| Class: | ELF32 |
| Data: | 2's complement, big endian |
| Version: | 1 (current) |
| Machine: | MIPS R3000 |
| Version Number: | 0x1 |
| Type: | EXEC (Executable file) |
| OS/ABI: | UNIX - System V |
| ABI Version: | 0 |
| Entry Point Address: | 0x400260 |
| Flags: | 0x1007 |
| ELF Header Size: | 52 |
| Program Header Offset: | 52 |
| Program Header Size: | 32 |

### ELF header

| | |
|---|---|
| Number of Program Headers: | 3 |
| Section Header Offset: | 100276 |
| Section Header Size: | 40 |
| Number of Section Headers: | 14 |
| Header String Table Index: | 13 |

### Sections

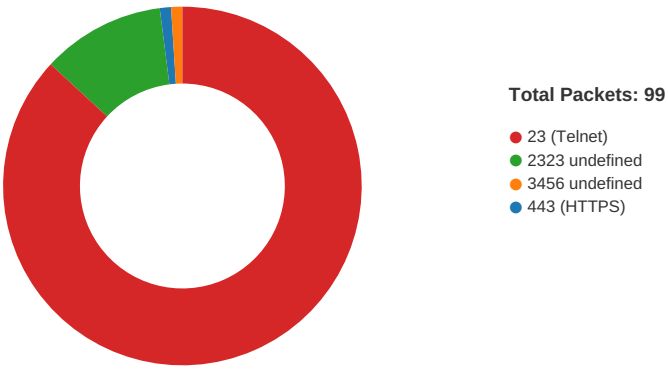
| Name | Type | Address | Offset | Size | EntSize | Flags | Flags Description | Link | Info | Align |
|---|---|---|---|---|---|---|---|---|---|---|
| | NULL | 0x0 | 0x0 | 0x0 | 0x0 | 0x0 | | 0 | 0 | 0 |
| .init | PROGBITS | 0x400094 | 0x94 | 0x8c | 0x0 | 0x6 | AX | 0 | 0 | 4 |
| .text | PROGBITS | 0x400120 | 0x120 | 0x15bc0 | 0x0 | 0x6 | AX | 0 | 0 | 16 |
| .fini | PROGBITS | 0x415ce0 | 0x15ce0 | 0x5c | 0x0 | 0x6 | AX | 0 | 0 | 4 |
| .rodata | PROGBITS | 0x415d40 | 0x15d40 | 0x1850 | 0x0 | 0x2 | A | 0 | 0 | 16 |
| .ctors | PROGBITS | 0x458000 | 0x18000 | 0x8 | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .dtors | PROGBITS | 0x458008 | 0x18008 | 0x8 | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .data.rel.ro | PROGBITS | 0x458014 | 0x18014 | 0x4 | 0x0 | 0x3 | WA | 0 | 0 | 4 |
| .data | PROGBITS | 0x458020 | 0x18020 | 0x300 | 0x0 | 0x3 | WA | 0 | 0 | 16 |
| .got | PROGBITS | 0x458320 | 0x18320 | 0x430 | 0x4 | 0x10000003 | WA | 0 | 0 | 16 |
| .sbss | NOBITS | 0x458750 | 0x18750 | 0x24 | 0x0 | 0x10000003 | WA | 0 | 0 | 4 |
| .bss | NOBITS | 0x458780 | 0x18750 | 0x2388 | 0x0 | 0x3 | WA | 0 | 0 | 16 |
| .mdebug.abi32 | PROGBITS | 0x8ca | 0x18750 | 0x0 | 0x0 | 0x0 | | 0 | 0 | 1 |
| .shstrtab | STRTAB | 0x0 | 0x18750 | 0x64 | 0x0 | 0x0 | | 0 | 0 | 1 |

### Program Segments

| Type | Offset | Virtual Address | Physical Address | File Size | Memory Size | Entropy | Flags | Flags Description | Align | Prog Interpreter | Section Mappings |
|---|---|---|---|---|---|---|---|---|---|---|---|
| LOAD | 0x0 | 0x400000 | 0x400000 | 0x17590 | 0x17590 | 3.5663 | 0x5 | R E | 0x10000 | | .init .text .fini .rodata |
| LOAD | 0x18000 | 0x458000 | 0x458000 | 0x750 | 0x2b08 | 2.3245 | 0x6 | RW | 0x10000 | | .ctors .dtors .data.rel.ro .data .got .sbss .bss |
| GNU_STACK | 0x0 | 0x0 | 0x0 | 0x0 | 0x0 | 0.0000 | 0x7 | RWE | 0x4 | | |

# Network Behavior

## Network Port Distribution




### TCP Packets

# System Behavior

## Analysis Process: 8PRjJeUifB PID: 5305 Parent PID: 5181

### General

| | |
|---|---|
| Start time: | 23:39:26 |
| Start date: | 01/11/2021 |
| Path: | /tmp/8PRjJeUifB |
| Arguments: | /tmp/8PRjJeUifB |
| File size: | 5777432 bytes |
| MD5 hash: | 0083f1f0e77be34ad27f849842bbb00c |

### File Activities

#### File Deleted

#### File Read

## Analysis Process: 8PRjJeUifB PID: 5309 Parent PID: 5305

### General

| | |
|---|---|
| Start time: | 23:39:28 |
| Start date: | 01/11/2021 |
| Path: | /tmp/8PRjJeUifB |
| Arguments: | n/a |
| File size: | 5777432 bytes |
| MD5 hash: | 0083f1f0e77be34ad27f849842bbb00c |

### File Activities

#### File Read

#### Directory Enumerated

## Analysis Process: 8PRjJeUifB PID: 5310 Parent PID: 5305

### General

| | |
|---|---|
| Start time: | 23:39:28 |
| Start date: | 01/11/2021 |
| Path: | /tmp/8PRjJeUifB |
| Arguments: | n/a |
| File size: | 5777432 bytes |
| MD5 hash: | 0083f1f0e77be34ad27f849842bbb00c |

## Analysis Process: 8PRjJeUifB PID: 5312 Parent PID: 5305

### General

| | |
|---|---|
| Start time: | 23:39:28 |
| Start date: | 01/11/2021 |
| Path: | /tmp/8PRjJeUifB |
| Arguments: | n/a |
| File size: | 5777432 bytes |
| MD5 hash: | 0083f1f0e77be34ad27f849842bbb00c |

## Analysis Process: systemd PID: 5316 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 23:39:30 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: journalctl PID: 5316 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 23:39:30 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/journalctl |
| Arguments: | /usr/bin/journalctl --smart-relinquish-var |
| File size: | 80120 bytes |
| MD5 hash: | bf3a987344f3bacafc44efd882abda8b |

### File Activities

#### File Read

## Analysis Process: systemd PID: 5327 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 23:39:30 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: systemd-journald PID: 5327 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 23:39:30 |
| Start date: | 01/11/2021 |
| Path: | /lib/systemd/systemd-journald |
| Arguments: | /lib/systemd/systemd-journald |
| File size: | 162032 bytes |
| MD5 hash: | 474667ece6cecb5e04c6eb897a1d0d9e |

### File Activities

#### File Deleted

#### File Read

File Written

File Moved

Directory Enumerated

Directory Created

## Analysis Process: systemd PID: 5334 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 23:39:34 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: journalctl PID: 5334 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 23:39:34 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/journalctl |
| Arguments: | /usr/bin/journalctl --flush |
| File size: | 80120 bytes |
| MD5 hash: | bf3a987344f3bacafc44efd882abda8b |

### File Activities

File Read

## Analysis Process: gdm3 PID: 5364 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 23:40:20 |
| Start date: | 01/11/2021 |
| Path: | /usr/sbin/gdm3 |
| Arguments: | n/a |
| File size: | 453296 bytes |
| MD5 hash: | 2492e2d8d34f9377e3e530a61a15674f |

## Analysis Process: Default PID: 5364 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 23:40:20 |
| Start date: | 01/11/2021 |
| Path: | /etc/gdm3/PrimeOff/Default |
| Arguments: | /etc/gdm3/PrimeOff/Default |
| File size: | 129816 bytes |

| | |
|---|---|
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

### File Activities

#### File Read

## Analysis Process: gdm3 PID: 5380 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 23:40:20 |
| Start date: | 01/11/2021 |
| Path: | /usr/sbin/gdm3 |
| Arguments: | n/a |
| File size: | 453296 bytes |
| MD5 hash: | 2492e2d8d34f9377e3e530a61a15674f |

## Analysis Process: Default PID: 5380 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 23:40:20 |
| Start date: | 01/11/2021 |
| Path: | /etc/gdm3/PrimeOff/Default |
| Arguments: | /etc/gdm3/PrimeOff/Default |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

### File Activities

#### File Read

## Analysis Process: systemd PID: 5387 Parent PID: 1860

### General

| | |
|---|---|
| Start time: | 23:40:37 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: pulseaudio PID: 5387 Parent PID: 1860

### General

| | |
|---|---|
| Start time: | 23:40:37 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/pulseaudio |
| Arguments: | /usr/bin/pulseaudio --daemonize=no --log-target=journal |
| File size: | 100832 bytes |
| MD5 hash: | 0c3b4c789d8ffb12b25507f27e14c186 |

### File Activities

File Deleted

File Read

File Written

Directory Enumerated

Directory Created

## Analysis Process: systemd PID: 5395 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 23:40:41 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: accounts-daemon PID: 5395 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 23:40:41 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/accountsservice/accounts-daemon |
| Arguments: | /usr/lib/accountsservice/accounts-daemon |
| File size: | 203192 bytes |
| MD5 hash: | 01a899e3fb5e7e434bea1290255a1f30 |

### File Activities

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Permission Modified

## Analysis Process: accounts-daemon PID: 5409 Parent PID: 5395

### General

| | |
|---|---|
| Start time: | 23:40:42 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/accountsservice/accounts-daemon |
| Arguments: | n/a |

| | |
|---|---|
| File size: | 203192 bytes |
| MD5 hash: | 01a899e3fb5e7e434bea1290255a1f30 |

### File Activities

#### Directory Enumerated

## Analysis Process: language-validate PID: 5409 Parent PID: 5395

### General

| | |
|---|---|
| Start time: | 23:40:42 |
| Start date: | 01/11/2021 |
| Path: | /usr/share/language-tools/language-validate |
| Arguments: | /usr/share/language-tools/language-validate en_US.UTF-8 |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

### File Activities

#### File Read

## Analysis Process: language-validate PID: 5410 Parent PID: 5409

### General

| | |
|---|---|
| Start time: | 23:40:42 |
| Start date: | 01/11/2021 |
| Path: | /usr/share/language-tools/language-validate |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: language-options PID: 5410 Parent PID: 5409

### General

| | |
|---|---|
| Start time: | 23:40:42 |
| Start date: | 01/11/2021 |
| Path: | /usr/share/language-tools/language-options |
| Arguments: | /usr/share/language-tools/language-options |
| File size: | 3478464 bytes |
| MD5 hash: | 16a21f464119ea7fad1d3660de963637 |

### File Activities

#### File Read

#### Directory Enumerated

## Analysis Process: language-options PID: 5413 Parent PID: 5410

### General

| | |
|---|---|
| Start time: | 23:40:42 |
| Start date: | 01/11/2021 |
| Path: | /usr/share/language-tools/language-options |
| Arguments: | n/a |
| File size: | 3478464 bytes |
| MD5 hash: | 16a21f464119ea7fad1d3660de963637 |

## Analysis Process: sh PID: 5413 Parent PID: 5410

### General

| | |
|---|---|
| Start time: | 23:40:42 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | sh -c "locale -a \| grep -F .utf8 " |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

### File Activities

#### File Read

## Analysis Process: sh PID: 5414 Parent PID: 5413

### General

| | |
|---|---|
| Start time: | 23:40:43 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: locale PID: 5414 Parent PID: 5413

### General

| | |
|---|---|
| Start time: | 23:40:43 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/locale |
| Arguments: | locale -a |
| File size: | 58944 bytes |
| MD5 hash: | c72a78792469db86d91369c9057f20d2 |

### File Activities

#### File Read

#### Directory Enumerated

## Analysis Process: sh PID: 5415 Parent PID: 5413

### General

| | |
|---|---|
| Start time: | 23:40:43 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: grep PID: 5415 Parent PID: 5413

### General

| | |
|---|---|
| Start time: | 23:40:43 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/grep |
| Arguments: | grep -F .utf8 |
| File size: | 199136 bytes |
| MD5 hash: | 1e6ebb9dd094f774478f72727bdba0f5 |

### File Activities

#### File Read

## Analysis Process: gdm-session-worker PID: 5405 Parent PID: 1809

### General

| | |
|---|---|
| Start time: | 23:40:41 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/gdm3/gdm-session-worker |
| Arguments: | n/a |
| File size: | 293360 bytes |
| MD5 hash: | 692243754bd9f38fe9bd7e230b5c060a |

## Analysis Process: Default PID: 5405 Parent PID: 1809

### General

| | |
|---|---|
| Start time: | 23:40:41 |
| Start date: | 01/11/2021 |
| Path: | /etc/gdm3/PostSession/Default |
| Arguments: | /etc/gdm3/PostSession/Default |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

### File Activities

#### File Read

## Analysis Process: gdm3 PID: 5416 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 23:40:44 |
| Start date: | 01/11/2021 |
| Path: | /usr/sbin/gdm3 |

| | |
|---|---|
| Arguments: | n/a |
| File size: | 453296 bytes |
| MD5 hash: | 2492e2d8d34f9377e3e530a61a15674f |

## Analysis Process: gdm-session-worker PID: 5416 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 23:40:44 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/gdm3/gdm-session-worker |
| Arguments: | "gdm-session-worker [pam/gdm-launch-environment]" |
| File size: | 293360 bytes |
| MD5 hash: | 692243754bd9f38fe9bd7e230b5c060a |

### File Activities

#### File Read

#### File Written

#### Directory Enumerated

## Analysis Process: gdm-session-worker PID: 5425 Parent PID: 5416

### General

| | |
|---|---|
| Start time: | 23:40:46 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/gdm3/gdm-session-worker |
| Arguments: | n/a |
| File size: | 293360 bytes |
| MD5 hash: | 692243754bd9f38fe9bd7e230b5c060a |

## Analysis Process: gdm-wayland-session PID: 5425 Parent PID: 5416

### General

| | |
|---|---|
| Start time: | 23:40:46 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/gdm3/gdm-wayland-session |
| Arguments: | /usr/lib/gdm3/gdm-wayland-session "dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart" |
| File size: | 76368 bytes |
| MD5 hash: | d3def63cf1e83f7fb8a0f13b1744ff7c |

### File Activities

#### File Read

## Analysis Process: gdm-wayland-session PID: 5430 Parent PID: 5425

### General

| | |
|---|---|
| Start time: | 23:40:46 |

| | |
|---|---|
| Start date: | 01/11/2021 |
| Path: | /usr/lib/gdm3/gdm-wayland-session |
| Arguments: | n/a |
| File size: | 76368 bytes |
| MD5 hash: | d3def63cf1e83f7fb8a0f13b1744ff7c |

#### File Activities

##### Directory Enumerated

## Analysis Process: dbus-run-session PID: 5430 Parent PID: 5425

#### General

| | |
|---|---|
| Start time: | 23:40:46 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-run-session |
| Arguments: | dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart |
| File size: | 14480 bytes |
| MD5 hash: | 245f3ef6a268850b33b0225a8753b7f4 |

#### File Activities

##### File Read

## Analysis Process: dbus-run-session PID: 5431 Parent PID: 5430

#### General

| | |
|---|---|
| Start time: | 23:40:46 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-run-session |
| Arguments: | n/a |
| File size: | 14480 bytes |
| MD5 hash: | 245f3ef6a268850b33b0225a8753b7f4 |

## Analysis Process: dbus-daemon PID: 5431 Parent PID: 5430

#### General

| | |
|---|---|
| Start time: | 23:40:46 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | dbus-daemon --nofork --print-address 4 --session |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

#### File Activities

##### File Read

##### Directory Enumerated

##### Directory Created

## Analysis Process: dbus-daemon PID: 5437 Parent PID: 5431

### General

| | |
|---|---|
| Start time: | 23:40:48 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5438 Parent PID: 5437

### General

| | |
|---|---|
| Start time: | 23:40:48 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

#### File Written

## Analysis Process: false PID: 5438 Parent PID: 5437

### General

| | |
|---|---|
| Start time: | 23:40:48 |
| Start date: | 01/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

### File Activities

#### File Read

## Analysis Process: dbus-daemon PID: 5440 Parent PID: 5431

### General

| | |
|---|---|
| Start time: | 23:40:48 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5441 Parent PID: 5440

### General

| | |
|---|---|
| Start time: | 23:40:48 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

#### File Activities

##### File Written

## Analysis Process: false PID: 5441 Parent PID: 5440

### General

| | |
|---|---|
| Start time: | 23:40:48 |
| Start date: | 01/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

#### File Activities

##### File Read

## Analysis Process: dbus-daemon PID: 5442 Parent PID: 5431

### General

| | |
|---|---|
| Start time: | 23:40:48 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5443 Parent PID: 5442

### General

| | |
|---|---|
| Start time: | 23:40:48 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

#### File Activities

##### File Written

## Analysis Process: false PID: 5443 Parent PID: 5442

### General

| | |
|---|---|
| Start time: | 23:40:48 |
| Start date: | 01/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

### File Activities

#### File Read

## Analysis Process: dbus-daemon PID: 5444 Parent PID: 5431

### General

| | |
|---|---|
| Start time: | 23:40:48 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5445 Parent PID: 5444

### General

| | |
|---|---|
| Start time: | 23:40:48 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

#### File Written

## Analysis Process: false PID: 5445 Parent PID: 5444

### General

| | |
|---|---|
| Start time: | 23:40:48 |
| Start date: | 01/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

### File Activities

#### File Read

## Analysis Process: dbus-daemon PID: 5446 Parent PID: 5431

### General

| | |
|---|---|
| Start time: | 23:40:49 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5447 Parent PID: 5446

### General

| | |
|---|---|
| Start time: | 23:40:49 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

#### File Written

## Analysis Process: false PID: 5447 Parent PID: 5446

### General

| | |
|---|---|
| Start time: | 23:40:49 |
| Start date: | 01/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

### File Activities

#### File Read

## Analysis Process: dbus-daemon PID: 5448 Parent PID: 5431

### General

| | |
|---|---|
| Start time: | 23:40:49 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5449 Parent PID: 5448

### General

| | |
|---|---|
| Start time: | 23:40:49 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

#### File Activities

##### File Written

## Analysis Process: false PID: 5449 Parent PID: 5448

### General

| | |
|---|---|
| Start time: | 23:40:49 |
| Start date: | 01/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

#### File Activities

##### File Read

## Analysis Process: dbus-daemon PID: 5451 Parent PID: 5431

### General

| | |
|---|---|
| Start time: | 23:40:50 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5452 Parent PID: 5451

### General

| | |
|---|---|
| Start time: | 23:40:50 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

#### File Activities

##### File Written

## Analysis Process: false PID: 5452 Parent PID: 5451

### General

| | |
|---|---|
| Start time: | 23:40:50 |
| Start date: | 01/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

### File Activities

#### File Read

## Analysis Process: dbus-run-session PID: 5434 Parent PID: 5430

### General

| | |
|---|---|
| Start time: | 23:40:47 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-run-session |
| Arguments: | n/a |
| File size: | 14480 bytes |
| MD5 hash: | 245f3ef6a268850b33b0225a8753b7f4 |

## Analysis Process: gnome-session PID: 5434 Parent PID: 5430

### General

| | |
|---|---|
| Start time: | 23:40:47 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/gnome-session |
| Arguments: | gnome-session --autostart /usr/share/gdm/greeter/autostart |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

### File Activities

#### File Read

## Analysis Process: gnome-session-binary PID: 5434 Parent PID: 5430

### General

| | |
|---|---|
| Start time: | 23:40:47 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

### File Activities

#### File Created

File Deleted

File Read

File Written

Directory Enumerated

Directory Created

Link Created

## Analysis Process: gnome-session-binary PID: 5453 Parent PID: 5434

### General

| | |
|---|---|
| Start time: | 23:40:50 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

### File Activities

Directory Enumerated

## Analysis Process: session-migration PID: 5453 Parent PID: 5434

### General

| | |
|---|---|
| Start time: | 23:40:50 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/session-migration |
| Arguments: | session-migration |
| File size: | 22680 bytes |
| MD5 hash: | 5227af42ebf14ac2fe2acddb002f68dc |

### File Activities

File Read

## Analysis Process: gnome-session-binary PID: 5454 Parent PID: 5434

### General

| | |
|---|---|
| Start time: | 23:40:50 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

### File Activities

Directory Enumerated

## Analysis Process: sh PID: 5454 Parent PID: 5434

### General

| | |
|---|---|
| Start time: | 23:40:50 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

### File Activities

File Read

## Analysis Process: gnome-shell PID: 5454 Parent PID: 5434

### General

| | |
|---|---|
| Start time: | 23:40:50 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/gnome-shell |
| Arguments: | /usr/bin/gnome-shell |
| File size: | 23168 bytes |
| MD5 hash: | da7a257239677622fe4b3a65972c9e87 |

### File Activities

File Read

Directory Enumerated

## Analysis Process: gdm3 PID: 5417 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 23:40:44 |
| Start date: | 01/11/2021 |
| Path: | /usr/sbin/gdm3 |
| Arguments: | n/a |
| File size: | 453296 bytes |
| MD5 hash: | 2492e2d8d34f9377e3e530a61a15674f |

## Analysis Process: Default PID: 5417 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 23:40:44 |
| Start date: | 01/11/2021 |
| Path: | /etc/gdm3/PrimeOff/Default |
| Arguments: | /etc/gdm3/PrimeOff/Default |
| File size: | 129816 bytes |

| | |
|---|---|
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

### File Activities

#### File Read

## Analysis Process: gdm3 PID: 5479 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 23:40:54 |
| Start date: | 01/11/2021 |
| Path: | /usr/sbin/gdm3 |
| Arguments: | n/a |
| File size: | 453296 bytes |
| MD5 hash: | 2492e2d8d34f9377e3e530a61a15674f |

## Analysis Process: gdm-session-worker PID: 5479 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 23:40:54 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/gdm3/gdm-session-worker |
| Arguments: | "gdm-session-worker [pam/gdm-launch-environment]" |
| File size: | 293360 bytes |
| MD5 hash: | 692243754bd9f38fe9bd7e230b5c060a |

### File Activities

#### File Read

#### File Written

#### Directory Enumerated

## Analysis Process: gdm-session-worker PID: 5484 Parent PID: 5479

### General

| | |
|---|---|
| Start time: | 23:40:56 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/gdm3/gdm-session-worker |
| Arguments: | n/a |
| File size: | 293360 bytes |
| MD5 hash: | 692243754bd9f38fe9bd7e230b5c060a |

## Analysis Process: gdm-x-session PID: 5484 Parent PID: 5479

### General

| | |
|---|---|
| Start time: | 23:40:56 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/gdm3/gdm-x-session |

| | |
|---|---|
| Arguments: | /usr/lib/gdm3/gdm-x-session "dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart" |
| File size: | 96944 bytes |
| MD5 hash: | 498a824333f1c1ec7767f4612d1887cc |

#### File Activities

#### File Read

#### File Written

#### Directory Created

## Analysis Process: gdm-x-session PID: 5486 Parent PID: 5484

### General

| | |
|---|---|
| Start time: | 23:40:56 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/gdm3/gdm-x-session |
| Arguments: | n/a |
| File size: | 96944 bytes |
| MD5 hash: | 498a824333f1c1ec7767f4612d1887cc |

#### File Activities

#### Directory Enumerated

## Analysis Process: Xorg PID: 5486 Parent PID: 5484

### General

| | |
|---|---|
| Start time: | 23:40:56 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/Xorg |
| Arguments: | /usr/bin/Xorg vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeptty -verbose 3 |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

#### File Activities

#### File Read

## Analysis Process: Xorg.wrap PID: 5486 Parent PID: 5484

### General

| | |
|---|---|
| Start time: | 23:40:56 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/xorg/Xorg.wrap |
| Arguments: | /usr/lib/xorg/Xorg.wrap vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeptty -verbose 3 |
| File size: | 14488 bytes |
| MD5 hash: | 48993830888200ecf19dd7def0884dfd |

#### File Activities

#### File Read

## Analysis Process: Xorg PID: 5486 Parent PID: 5484

### General

| | |
|---|---|
| Start time: | 23:40:56 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/xorg/Xorg |
| Arguments: | /usr/lib/xorg/Xorg vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeptty -verbose 3 |
| File size: | 2448840 bytes |
| MD5 hash: | 730cf4c45a7ee8bea88abf165463b7f8 |

### File Activities

#### File Deleted

#### File Read

#### File Written

#### File Moved

#### Directory Enumerated

## Analysis Process: Xorg PID: 5519 Parent PID: 5486

### General

| | |
|---|---|
| Start time: | 23:41:06 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/xorg/Xorg |
| Arguments: | n/a |
| File size: | 2448840 bytes |
| MD5 hash: | 730cf4c45a7ee8bea88abf165463b7f8 |

## Analysis Process: sh PID: 5519 Parent PID: 5486

### General

| | |
|---|---|
| Start time: | 23:41:06 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | sh -c "\"/usr/bin/xkbcomp\" -w 1 \"-R/usr/share/X11/xkb\" -xkm \"-\" -em1 \"The XKEYBOARD keymap compiler (xkbcomp) reports:\" -emp \"> \" -eml \"Errors from xkbcomp are not fatal to the X server\" \"/tmp/server-0.xkm\"" |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

### File Activities

#### File Read

## Analysis Process: sh PID: 5520 Parent PID: 5519

### General

| | |
|---|---|
| Start time: | 23:41:07 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: xkbcomp PID: 5520 Parent PID: 5519

### General

| | |
|---|---|
| Start time: | 23:41:07 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/xkbcomp |
| Arguments: | /usr/bin/xkbcomp -w 1 -R/usr/share/X11/xkb -xkm - -em1 "The XKEYBOARD keymap compiler (xkbcomp) reports:" -emp "> " -eml "Errors from xkbcomp are not fatal to the X server" /tmp/server-0.xkm |
| File size: | 217184 bytes |
| MD5 hash: | c5f953aec4c00d2a1cc27acb75d62c9b |

### File Activities

#### File Deleted

#### File Read

#### File Written

## Analysis Process: Xorg PID: 5897 Parent PID: 5486

### General

| | |
|---|---|
| Start time: | 23:41:40 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/xorg/Xorg |
| Arguments: | n/a |
| File size: | 2448840 bytes |
| MD5 hash: | 730cf4c45a7ee8bea88abf165463b7f8 |

## Analysis Process: sh PID: 5897 Parent PID: 5486

### General

| | |
|---|---|
| Start time: | 23:41:40 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | sh -c "\"/usr/bin/xkbcomp\" -w 1 \"-R/usr/share/X11/xkb\" -xkm \"-\" -em1 \"The XKEYBOARD keymap compiler (xkbcomp) reports:\" -emp \"> \" -eml \"Errors from xkbcomp are not fatal to the X server\" \"/tmp/server-0.xkm\"" |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

### File Activities

#### File Read

## Analysis Process: sh PID: 5900 Parent PID: 5897

### General

| | |
|---|---|
| Start time: | 23:41:40 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | n/a |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: xkbcomp PID: 5900 Parent PID: 5897

### General

| | |
|---|---|
| Start time: | 23:41:40 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/xkbcomp |
| Arguments: | /usr/bin/xkbcomp -w 1 -R/usr/share/X11/xkb -xkm - -em1 "The XKEYBOARD keymap compiler (xkbcomp) reports:" -emp "> " -eml "Errors from xkbcomp are not fatal to the X server" /tmp/server-0.xkm |
| File size: | 217184 bytes |
| MD5 hash: | c5f953aec4c00d2a1cc27acb75d62c9b |

### File Activities

#### File Deleted

#### File Read

#### File Written

## Analysis Process: gdm-x-session PID: 5528 Parent PID: 5484

### General

| | |
|---|---|
| Start time: | 23:41:11 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/gdm3/gdm-x-session |
| Arguments: | n/a |
| File size: | 96944 bytes |
| MD5 hash: | 498a824333f1c1ec7767f4612d1887cc |

### File Activities

#### Directory Enumerated

## Analysis Process: Default PID: 5528 Parent PID: 5484

### General

| | |
|---|---|
| Start time: | 23:41:12 |
| Start date: | 01/11/2021 |
| Path: | /etc/gdm3/Prime/Default |
| Arguments: | /etc/gdm3/Prime/Default |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

### File Activities

File Read

## Analysis Process: gdm-x-session PID: 5529 Parent PID: 5484

### General

| | |
|---|---|
| Start time: | 23:41:12 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/gdm3/gdm-x-session |
| Arguments: | n/a |
| File size: | 96944 bytes |
| MD5 hash: | 498a824333f1c1ec7767f4612d1887cc |

### File Activities

File Read

## Analysis Process: dbus-run-session PID: 5529 Parent PID: 5484

### General

| | |
|---|---|
| Start time: | 23:41:12 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-run-session |
| Arguments: | dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart |
| File size: | 14480 bytes |
| MD5 hash: | 245f3ef6a268850b33b0225a8753b7f4 |

### File Activities

File Read

## Analysis Process: dbus-run-session PID: 5530 Parent PID: 5529

### General

| | |
|---|---|
| Start time: | 23:41:12 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-run-session |
| Arguments: | n/a |
| File size: | 14480 bytes |
| MD5 hash: | 245f3ef6a268850b33b0225a8753b7f4 |

## Analysis Process: dbus-daemon PID: 5530 Parent PID: 5529

### General

| | |
|---|---|
| Start time: | 23:41:12 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | dbus-daemon --nofork --print-address 4 --session |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

#### File Read

#### Directory Enumerated

#### Directory Created

## Analysis Process: dbus-daemon PID: 5546 Parent PID: 5530

### General

| | |
|---|---|
| Start time: | 23:41:20 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5547 Parent PID: 5546

### General

| | |
|---|---|
| Start time: | 23:41:20 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

#### File Written

## Analysis Process: at-spi-bus-launcher PID: 5547 Parent PID: 5546

### General

| | |
|---|---|
| Start time: | 23:41:20 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/at-spi-bus-launcher |
| Arguments: | /usr/libexec/at-spi-bus-launcher |
| File size: | 27008 bytes |
| MD5 hash: | 1563f274acd4e7ba530a55bdc4c95682 |

### File Activities

#### File Read

#### File Written

#### Directory Enumerated

#### Directory Created

## Analysis Process: at-spi-bus-launcher PID: 5552 Parent PID: 5547

### General

| | |
|---|---|
| Start time: | 23:41:20 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/at-spi-bus-launcher |
| Arguments: | n/a |
| File size: | 27008 bytes |
| MD5 hash: | 1563f274acd4e7ba530a55bdc4c95682 |

### File Activities

#### Directory Enumerated

## Analysis Process: dbus-daemon PID: 5552 Parent PID: 5547

### General

| | |
|---|---|
| Start time: | 23:41:20 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | /usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2/accessibility.conf --nofork --print-address 3 |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

#### File Read

#### Directory Enumerated

## Analysis Process: dbus-daemon PID: 6116 Parent PID: 5552

### General

| | |
|---|---|
| Start time: | 23:41:44 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 6117 Parent PID: 6116

### General

| | |
|---|---|
| Start time: | 23:41:44 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

File Written

## Analysis Process: at-spi2-registryd PID: 6117 Parent PID: 6116

### General

| | |
|---|---|
| Start time: | 23:41:44 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/at-spi2-registryd |
| Arguments: | /usr/libexec/at-spi2-registryd --use-gnome-session |
| File size: | 100224 bytes |
| MD5 hash: | 1d904c2693452edebc7ede3a9e24d440 |

### File Activities

File Read

## Analysis Process: dbus-daemon PID: 5576 Parent PID: 5530

### General

| | |
|---|---|
| Start time: | 23:41:22 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5577 Parent PID: 5576

### General

| | |
|---|---|
| Start time: | 23:41:22 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

File Written

## Analysis Process: false PID: 5577 Parent PID: 5576

### General

| | |
|---|---|
| Start time: | 23:41:22 |
| Start date: | 01/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

### File Activities

#### File Read

## Analysis Process: dbus-daemon PID: 5579 Parent PID: 5530

### General

| | |
|---|---|
| Start time: | 23:41:23 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5580 Parent PID: 5579

### General

| | |
|---|---|
| Start time: | 23:41:23 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

#### File Written

## Analysis Process: false PID: 5580 Parent PID: 5579

### General

| | |
|---|---|
| Start time: | 23:41:23 |
| Start date: | 01/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

### File Activities

#### File Read

## Analysis Process: dbus-daemon PID: 5581 Parent PID: 5530

### General

| | |
|---|---|
| Start time: | 23:41:23 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |

| | |
|---|---|
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5582 Parent PID: 5581

### General

| | |
|---|---|
| Start time: | 23:41:23 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

#### File Written

## Analysis Process: false PID: 5582 Parent PID: 5581

### General

| | |
|---|---|
| Start time: | 23:41:23 |
| Start date: | 01/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

### File Activities

#### File Read

## Analysis Process: dbus-daemon PID: 5583 Parent PID: 5530

### General

| | |
|---|---|
| Start time: | 23:41:23 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5584 Parent PID: 5583

### General

| | |
|---|---|
| Start time: | 23:41:23 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

### File Written

## Analysis Process: false PID: 5584 Parent PID: 5583

### General

| | |
|---|---|
| Start time: | 23:41:23 |
| Start date: | 01/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

### File Activities

### File Read

## Analysis Process: dbus-daemon PID: 5585 Parent PID: 5530

### General

| | |
|---|---|
| Start time: | 23:41:23 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5586 Parent PID: 5585

### General

| | |
|---|---|
| Start time: | 23:41:23 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

### File Written

## Analysis Process: false PID: 5586 Parent PID: 5585

### General

| | |
|---|---|
| Start time: | 23:41:23 |
| Start date: | 01/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

### File Activities

#### File Read

## Analysis Process: dbus-daemon PID: 5587 Parent PID: 5530

### General

| | |
|---|---|
| Start time: | 23:41:24 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5588 Parent PID: 5587

### General

| | |
|---|---|
| Start time: | 23:41:24 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

#### File Written

## Analysis Process: false PID: 5588 Parent PID: 5587

### General

| | |
|---|---|
| Start time: | 23:41:24 |
| Start date: | 01/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

### File Activities

#### File Read

## Analysis Process: dbus-daemon PID: 5590 Parent PID: 5530

### General

| | |
|---|---|
| Start time: | 23:41:24 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |

| | |
|---|---|
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5591 Parent PID: 5590

### General

| | |
|---|---|
| Start time: | 23:41:24 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

#### File Written

## Analysis Process: false PID: 5591 Parent PID: 5590

### General

| | |
|---|---|
| Start time: | 23:41:24 |
| Start date: | 01/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

### File Activities

#### File Read

## Analysis Process: dbus-daemon PID: 5894 Parent PID: 5530

### General

| | |
|---|---|
| Start time: | 23:41:39 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 5895 Parent PID: 5894

### General

| | |
|---|---|
| Start time: | 23:41:39 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

File Written

## Analysis Process: ibus-portal PID: 5895 Parent PID: 5894

### General

| | |
|---|---|
| Start time: | 23:41:40 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/ibus-portal |
| Arguments: | /usr/libexec/ibus-portal |
| File size: | 92536 bytes |
| MD5 hash: | 562ad55bd9a4d54bd7b76746b01e37d3 |

### File Activities

File Read

Directory Enumerated

Directory Created

## Analysis Process: dbus-daemon PID: 6123 Parent PID: 5530

### General

| | |
|---|---|
| Start time: | 23:41:44 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 6124 Parent PID: 6123

### General

| | |
|---|---|
| Start time: | 23:41:44 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

### File Activities

File Written

## Analysis Process: gjs PID: 6124 Parent PID: 6123

### General

| | |
|---|---|
| Start time: | 23:41:44 |
| Start date: | 01/11/2021 |

| | |
|---|---|
| Path: | /usr/bin/gjs |
| Arguments: | /usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications |
| File size: | 23128 bytes |
| MD5 hash: | 5f3eceb792bb65c22f23d1efb4fde3ad |

#### File Activities

##### File Read

##### Directory Enumerated

## Analysis Process: dbus-daemon PID: 6185 Parent PID: 5530

#### General

| | |
|---|---|
| Start time: | 23:41:58 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

## Analysis Process: dbus-daemon PID: 6186 Parent PID: 6185

#### General

| | |
|---|---|
| Start time: | 23:41:58 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-daemon |
| Arguments: | n/a |
| File size: | 249032 bytes |
| MD5 hash: | 3089d47e3f3ab84cd81c48fd406d7a8c |

#### File Activities

##### File Written

## Analysis Process: false PID: 6186 Parent PID: 6185

#### General

| | |
|---|---|
| Start time: | 23:41:58 |
| Start date: | 01/11/2021 |
| Path: | /bin/false |
| Arguments: | /bin/false |
| File size: | 39256 bytes |
| MD5 hash: | 3177546c74e4f0062909eae43d948bfc |

#### File Activities

##### File Read

## Analysis Process: dbus-run-session PID: 5531 Parent PID: 5529

### General

| | |
|---|---|
| Start time: | 23:41:12 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/dbus-run-session |
| Arguments: | n/a |
| File size: | 14480 bytes |
| MD5 hash: | 245f3ef6a268850b33b0225a8753b7f4 |

## Analysis Process: gnome-session PID: 5531 Parent PID: 5529

### General

| | |
|---|---|
| Start time: | 23:41:12 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/gnome-session |
| Arguments: | gnome-session --autostart /usr/share/gdm/greeter/autostart |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

### File Activities

#### File Read

## Analysis Process: gnome-session-binary PID: 5531 Parent PID: 5529

### General

| | |
|---|---|
| Start time: | 23:41:12 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

### File Activities

#### File Created

#### File Deleted

#### File Read

#### File Written

#### Directory Enumerated

#### Directory Created

#### Link Created

## Analysis Process: gnome-session-binary PID: 5534 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:12 |

| | |
|---|---|
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

#### File Activities

##### Directory Enumerated

## Analysis Process: gnome-session-check-accelerated PID: 5534 Parent PID: 5531

#### General

| | |
|---|---|
| Start time: | 23:41:12 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-check-accelerated |
| Arguments: | /usr/libexec/gnome-session-check-accelerated |
| File size: | 18752 bytes |
| MD5 hash: | a64839518af85b2b9de31aca27646396 |

#### File Activities

##### File Read

##### Directory Enumerated

## Analysis Process: gnome-session-check-accelerated PID: 5553 Parent PID: 5534

#### General

| | |
|---|---|
| Start time: | 23:41:20 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-check-accelerated |
| Arguments: | n/a |
| File size: | 18752 bytes |
| MD5 hash: | a64839518af85b2b9de31aca27646396 |

#### File Activities

##### Directory Enumerated

## Analysis Process: gnome-session-check-accelerated-gl-helper PID: 5553 Parent PID: 5534

#### General

| | |
|---|---|
| Start time: | 23:41:20 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-check-accelerated-gl-helper |
| Arguments: | /usr/libexec/gnome-session-check-accelerated-gl-helper --print-renderer |
| File size: | 22920 bytes |
| MD5 hash: | b1ab9a384f9e98a39ae5c36037dd5e78 |

#### File Activities

File Read

Directory Enumerated

## Analysis Process: gnome-session-check-accelerated PID: 5563 Parent PID: 5534

### General

| | |
|---|---|
| Start time: | 23:41:21 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-check-accelerated |
| Arguments: | n/a |
| File size: | 18752 bytes |
| MD5 hash: | a64839518af85b2b9de31aca27646396 |

### File Activities

Directory Enumerated

## Analysis Process: gnome-session-check-accelerated-gles-helper PID: 5563 Parent PID: 5534

### General

| | |
|---|---|
| Start time: | 23:41:21 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-check-accelerated-gles-helper |
| Arguments: | /usr/libexec/gnome-session-check-accelerated-gles-helper --print-renderer |
| File size: | 14728 bytes |
| MD5 hash: | 1bd78885765a18e60c05ed1fb5fa3bf8 |

### File Activities

File Read

Directory Enumerated

## Analysis Process: gnome-session-binary PID: 5592 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:24 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

### File Activities

Directory Enumerated

## Analysis Process: session-migration PID: 5592 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:24 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/session-migration |
| Arguments: | session-migration |
| File size: | 22680 bytes |
| MD5 hash: | 5227af42ebf14ac2fe2acddb002f68dc |

#### File Activities

##### File Read

## Analysis Process: gnome-session-binary PID: 5593 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:25 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

#### File Activities

##### Directory Enumerated

## Analysis Process: sh PID: 5593 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:25 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

#### File Activities

##### File Read

## Analysis Process: gnome-shell PID: 5593 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:25 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/gnome-shell |
| Arguments: | /usr/bin/gnome-shell |
| File size: | 23168 bytes |
| MD5 hash: | da7a257239677622fe4b3a65972c9e87 |

#### File Activities

File Deleted

File Read

File Written

Directory Enumerated

Directory Created

## Analysis Process: gnome-shell PID: 5646 Parent PID: 5593

### General

| | |
|---|---|
| Start time: | 23:41:38 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/gnome-shell |
| Arguments: | n/a |
| File size: | 23168 bytes |
| MD5 hash: | da7a257239677622fe4b3a65972c9e87 |

### File Activities

Directory Enumerated

## Analysis Process: ibus-daemon PID: 5646 Parent PID: 5593

### General

| | |
|---|---|
| Start time: | 23:41:38 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/ibus-daemon |
| Arguments: | ibus-daemon --panel disable --xim |
| File size: | 199088 bytes |
| MD5 hash: | 1e00fb9860b198c73f6e364e3ff16f31 |

### File Activities

File Deleted

File Read

File Written

Directory Enumerated

Directory Created

## Analysis Process: ibus-daemon PID: 5890 Parent PID: 5646

### General

| | |
|---|---|
| Start time: | 23:41:39 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/ibus-daemon |

| | |
|---|---|
| Arguments: | n/a |
| File size: | 199088 bytes |
| MD5 hash: | 1e00fb9860b198c73f6e364e3ff16f31 |

#### File Activities

##### Directory Enumerated

## Analysis Process: ibus-memconf PID: 5890 Parent PID: 5646

#### General

| | |
|---|---|
| Start time: | 23:41:39 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/ibus-memconf |
| Arguments: | /usr/libexec/ibus-memconf |
| File size: | 22904 bytes |
| MD5 hash: | 523e939905910d06598e66385761a822 |

#### File Activities

##### File Read

##### Directory Enumerated

##### Directory Created

## Analysis Process: ibus-daemon PID: 5892 Parent PID: 5646

#### General

| | |
|---|---|
| Start time: | 23:41:39 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/ibus-daemon |
| Arguments: | n/a |
| File size: | 199088 bytes |
| MD5 hash: | 1e00fb9860b198c73f6e364e3ff16f31 |

## Analysis Process: ibus-daemon PID: 5893 Parent PID: 5892

#### General

| | |
|---|---|
| Start time: | 23:41:39 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/ibus-daemon |
| Arguments: | n/a |
| File size: | 199088 bytes |
| MD5 hash: | 1e00fb9860b198c73f6e364e3ff16f31 |

#### File Activities

##### Directory Enumerated

## Analysis Process: ibus-x11 PID: 5893 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 23:41:39 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/ibus-x11 |
| Arguments: | /usr/libexec/ibus-x11 --kill-daemon |
| File size: | 100352 bytes |
| MD5 hash: | 2aa1e54666191243814c2733d6992dbd |

#### File Activities

##### File Read

##### Directory Enumerated

##### Directory Created

## Analysis Process: ibus-daemon PID: 6168 Parent PID: 5646

### General

| | |
|---|---|
| Start time: | 23:41:53 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/ibus-daemon |
| Arguments: | n/a |
| File size: | 199088 bytes |
| MD5 hash: | 1e00fb9860b198c73f6e364e3ff16f31 |

#### File Activities

##### Directory Enumerated

## Analysis Process: ibus-engine-simple PID: 6168 Parent PID: 5646

### General

| | |
|---|---|
| Start time: | 23:41:54 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/ibus-engine-simple |
| Arguments: | /usr/libexec/ibus-engine-simple |
| File size: | 14712 bytes |
| MD5 hash: | 0238866d5e8802a0ce1b1b9af8cb1376 |

#### File Activities

##### File Read

##### Directory Enumerated

##### Directory Created

## Analysis Process: gnome-session-binary PID: 6140 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:48 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

#### File Activities

##### Directory Enumerated

## Analysis Process: sh PID: 6140 Parent PID: 5531

#### General

| | |
|---|---|
| Start time: | 23:41:48 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sharing |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

#### File Activities

##### File Read

## Analysis Process: gsd-sharing PID: 6140 Parent PID: 5531

#### General

| | |
|---|---|
| Start time: | 23:41:48 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gsd-sharing |
| Arguments: | /usr/libexec/gsd-sharing |
| File size: | 35424 bytes |
| MD5 hash: | e29d9025d98590fbb69f89fdbd4438b3 |

#### File Activities

##### File Read

##### File Written

##### Directory Enumerated

##### Directory Created

## Analysis Process: gnome-session-binary PID: 6142 Parent PID: 5531

#### General

| | |
|---|---|
| Start time: | 23:41:48 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |

| | |
|---|---|
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

### File Activities

#### Directory Enumerated

## Analysis Process: sh PID: 6142 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:48 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-wacom |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

### File Activities

#### File Read

## Analysis Process: gsd-wacom PID: 6142 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:48 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gsd-wacom |
| Arguments: | /usr/libexec/gsd-wacom |
| File size: | 39520 bytes |
| MD5 hash: | 13778dd1a23a4e94ddc17ac9caa4fcc1 |

### File Activities

#### File Read

#### Directory Enumerated

## Analysis Process: gnome-session-binary PID: 6144 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:48 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

### File Activities

#### Directory Enumerated

## Analysis Process: sh PID: 6144 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:48 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-color |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

### File Activities

#### File Read

## Analysis Process: gsd-color PID: 6144 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:49 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gsd-color |
| Arguments: | /usr/libexec/gsd-color |
| File size: | 92832 bytes |
| MD5 hash: | ac2861ad93ce047283e8e87cefef9a19 |

### File Activities

#### File Read

#### File Written

#### Directory Enumerated

#### Directory Created

## Analysis Process: gnome-session-binary PID: 6145 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:49 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

## Analysis Process: sh PID: 6145 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:49 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-keyboard |
| File size: | 129816 bytes |

| | |
|---|---|
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: gsd-keyboard PID: 6145 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:49 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gsd-keyboard |
| Arguments: | /usr/libexec/gsd-keyboard |
| File size: | 39760 bytes |
| MD5 hash: | 8e288fd17c80bb0a1148b964b2ac2279 |

## Analysis Process: gnome-session-binary PID: 6146 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:49 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

## Analysis Process: sh PID: 6146 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:50 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-print-notifications |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: gsd-print-notifications PID: 6146 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:50 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gsd-print-notifications |
| Arguments: | /usr/libexec/gsd-print-notifications |
| File size: | 51840 bytes |
| MD5 hash: | 71539698aa691718cee775d6b9450ae2 |

## Analysis Process: gsd-print-notifications PID: 6194 Parent PID: 6146

### General

| | |
|---|---|
| Start time: | 23:41:59 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gsd-print-notifications |

| | |
|---|---|
| Arguments: | n/a |
| File size: | 51840 bytes |
| MD5 hash: | 71539698aa691718cee775d6b9450ae2 |

## Analysis Process: gsd-print-notifications PID: 6195 Parent PID: 6194

### General

| | |
|---|---|
| Start time: | 23:41:59 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gsd-print-notifications |
| Arguments: | n/a |
| File size: | 51840 bytes |
| MD5 hash: | 71539698aa691718cee775d6b9450ae2 |

## Analysis Process: gsd-printer PID: 6195 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 23:41:59 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gsd-printer |
| Arguments: | /usr/libexec/gsd-printer |
| File size: | 31120 bytes |
| MD5 hash: | 7995828cf98c315fd55f2ffb3b22384d |

## Analysis Process: gnome-session-binary PID: 6147 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:50 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

## Analysis Process: sh PID: 6147 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:50 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-rfkill |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: gsd-rfkill PID: 6147 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:50 |

| | |
|---|---|
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gsd-rfkill |
| Arguments: | /usr/libexec/gsd-rfkill |
| File size: | 51808 bytes |
| MD5 hash: | 88a16a3c0aba1759358c06215ecfb5cc |

## Analysis Process: gnome-session-binary PID: 6148 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:50 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

## Analysis Process: sh PID: 6148 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:50 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-smartcard |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: gsd-smartcard PID: 6148 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:50 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gsd-smartcard |
| Arguments: | /usr/libexec/gsd-smartcard |
| File size: | 109152 bytes |
| MD5 hash: | ea1fbd7f62e4cd0331eae2ef754ee605 |

## Analysis Process: gnome-session-binary PID: 6150 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:50 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

## Analysis Process: sh PID: 6150 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:50 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-datetime |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: gsd-datetime PID: 6150 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:51 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gsd-datetime |
| Arguments: | /usr/libexec/gsd-datetime |
| File size: | 76736 bytes |
| MD5 hash: | d80d39745740de37d6634d36e344d4bc |

## Analysis Process: gnome-session-binary PID: 6151 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:51 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

## Analysis Process: sh PID: 6151 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:51 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-media-keys |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: gsd-media-keys PID: 6151 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:51 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gsd-media-keys |
| Arguments: | /usr/libexec/gsd-media-keys |
| File size: | 232936 bytes |
| MD5 hash: | a425448c135afb4b8bfd79cc0b6b74da |

## Analysis Process: gnome-session-binary PID: 6153 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:51 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

## Analysis Process: sh PID: 6153 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:51 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-screensaver-proxy |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: gsd-screensaver-proxy PID: 6153 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:52 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gsd-screensaver-proxy |
| Arguments: | /usr/libexec/gsd-screensaver-proxy |
| File size: | 27232 bytes |
| MD5 hash: | 77e309450c87dceee43f1a9e50cc0d02 |

## Analysis Process: gnome-session-binary PID: 6154 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:51 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

## Analysis Process: sh PID: 6154 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:52 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sound |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: gsd-sound PID: 6154 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:52 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gsd-sound |
| Arguments: | /usr/libexec/gsd-sound |
| File size: | 31248 bytes |
| MD5 hash: | 4c7d3fb993463337b4a0eb5c80c760ee |

## Analysis Process: gnome-session-binary PID: 6158 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:52 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

## Analysis Process: sh PID: 6158 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:52 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-a11y-settings |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: gsd-a11y-settings PID: 6158 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:53 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gsd-a11y-settings |
| Arguments: | /usr/libexec/gsd-a11y-settings |
| File size: | 23056 bytes |
| MD5 hash: | 18e243d2cf30ecee7ea89d1462725c5c |

## Analysis Process: gnome-session-binary PID: 6161 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:52 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

## Analysis Process: sh PID: 6161 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:53 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-housekeeping |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: gsd-housekeeping PID: 6161 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:54 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gsd-housekeeping |
| Arguments: | /usr/libexec/gsd-housekeeping |
| File size: | 51840 bytes |
| MD5 hash: | b55f3394a84976ddb92a2915e5d76914 |

## Analysis Process: gnome-session-binary PID: 6167 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:53 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

## Analysis Process: sh PID: 6167 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:54 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-power |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: gsd-power PID: 6167 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:41:54 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gsd-power |
| Arguments: | /usr/libexec/gsd-power |
| File size: | 88672 bytes |
| MD5 hash: | 28b8e1b43c3e7f1db6741ea1ecd978b7 |

## Analysis Process: gnome-session-binary PID: 7011 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:42:21 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

## Analysis Process: sh PID: 7011 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:42:22 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/spice-vdagent |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: spice-vdagent PID: 7011 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:42:22 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/spice-vdagent |
| Arguments: | /usr/bin/spice-vdagent |
| File size: | 80664 bytes |
| MD5 hash: | 80fb7f613aa78d1b8a229dbcf4577a9d |

## Analysis Process: gnome-session-binary PID: 7015 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:42:24 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gnome-session-binary |
| Arguments: | n/a |
| File size: | 334664 bytes |
| MD5 hash: | d9b90be4f7db60cb3c2d3da6a1d31bfb |

## Analysis Process: sh PID: 7015 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:42:24 |
| Start date: | 01/11/2021 |
| Path: | /bin/sh |
| Arguments: | /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh xbrlapi -q |
| File size: | 129816 bytes |

| | |
|---|---|
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: xbrlapi PID: 7015 Parent PID: 5531

### General

| | |
|---|---|
| Start time: | 23:42:24 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/xbrlapi |
| Arguments: | xbrlapi -q |
| File size: | 166384 bytes |
| MD5 hash: | 0cfe25df39d38af32d6265ed947ca5b9 |

## Analysis Process: gdm3 PID: 5480 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 23:40:54 |
| Start date: | 01/11/2021 |
| Path: | /usr/sbin/gdm3 |
| Arguments: | n/a |
| File size: | 453296 bytes |
| MD5 hash: | 2492e2d8d34f9377e3e530a61a15674f |

## Analysis Process: Default PID: 5480 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 23:40:54 |
| Start date: | 01/11/2021 |
| Path: | /etc/gdm3/PrimeOff/Default |
| Arguments: | /etc/gdm3/PrimeOff/Default |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: gdm3 PID: 5481 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 23:40:54 |
| Start date: | 01/11/2021 |
| Path: | /usr/sbin/gdm3 |
| Arguments: | n/a |
| File size: | 453296 bytes |
| MD5 hash: | 2492e2d8d34f9377e3e530a61a15674f |

## Analysis Process: Default PID: 5481 Parent PID: 1320

### General

| | |
|---|---|
| Start time: | 23:40:54 |
| Start date: | 01/11/2021 |
| Path: | /etc/gdm3/PrimeOff/Default |

| | |
|---|---|
| Arguments: | /etc/gdm3/PrimeOff/Default |
| File size: | 129816 bytes |
| MD5 hash: | 1e6b1c887c59a315edb7eb9a315fc84c |

## Analysis Process: gvfsd-fuse PID: 5490 Parent PID: 2038

### General

| | |
|---|---|
| Start time: | 23:41:01 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/gvfsd-fuse |
| Arguments: | n/a |
| File size: | 47632 bytes |
| MD5 hash: | d18fbf1cbf8eb57b17fac48b7b4be933 |

## Analysis Process: fusermount PID: 5490 Parent PID: 2038

### General

| | |
|---|---|
| Start time: | 23:41:01 |
| Start date: | 01/11/2021 |
| Path: | /bin/fusermount |
| Arguments: | fusermount -u -q -z -- /run/user/1000/gvfs |
| File size: | 39144 bytes |
| MD5 hash: | 576a1b135c82bdcbc97a91acea900566 |

## Analysis Process: systemd PID: 5506 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 23:41:02 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: systemd-user-runtime-dir PID: 5506 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 23:41:02 |
| Start date: | 01/11/2021 |
| Path: | /lib/systemd/systemd-user-runtime-dir |
| Arguments: | /lib/systemd/systemd-user-runtime-dir stop 1000 |
| File size: | 22672 bytes |
| MD5 hash: | d55f4b0847f88131dbcfb07435178e54 |

## Analysis Process: systemd PID: 5618 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 23:41:39 |

| | |
|---|---|
| Start date: | 01/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: systemd-localed PID: 5618 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 23:41:39 |
| Start date: | 01/11/2021 |
| Path: | /lib/systemd/systemd-localed |
| Arguments: | /lib/systemd/systemd-localed |
| File size: | 43232 bytes |
| MD5 hash: | 1244af9646256d49594f2a8203329aa9 |

## Analysis Process: systemd PID: 5906 Parent PID: 1334

### General

| | |
|---|---|
| Start time: | 23:41:41 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: pulseaudio PID: 5906 Parent PID: 1334

### General

| | |
|---|---|
| Start time: | 23:41:41 |
| Start date: | 01/11/2021 |
| Path: | /usr/bin/pulseaudio |
| Arguments: | /usr/bin/pulseaudio --daemonize=no --log-target=journal |
| File size: | 100832 bytes |
| MD5 hash: | 0c3b4c789d8ffb12b25507f27e14c186 |

## Analysis Process: systemd PID: 5907 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 23:41:42 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: geoclue PID: 5907 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 23:41:42 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/geoclue |
| Arguments: | /usr/libexec/geoclue |
| File size: | 301544 bytes |
| MD5 hash: | 30ac5455f3c598dde91dc87477fb19f7 |

## Analysis Process: systemd PID: 6196 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 23:42:00 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: systemd-hostnamed PID: 6196 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 23:42:00 |
| Start date: | 01/11/2021 |
| Path: | /lib/systemd/systemd-hostnamed |
| Arguments: | /lib/systemd/systemd-hostnamed |
| File size: | 35040 bytes |
| MD5 hash: | 2cc8a5576629a2d5bd98e49a4b8bef65 |

## Analysis Process: systemd PID: 6539 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 23:42:14 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: fprintd PID: 6539 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 23:42:14 |
| Start date: | 01/11/2021 |
| Path: | /usr/libexec/fprintd |
| Arguments: | /usr/libexec/fprintd |
| File size: | 125312 bytes |
| MD5 hash: | b0d8829f05cd028529b84b061b660e84 |

## Analysis Process: systemd PID: 6746 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 23:42:17 |
| Start date: | 01/11/2021 |
| Path: | /usr/lib/systemd/systemd |
| Arguments: | n/a |
| File size: | 1620224 bytes |
| MD5 hash: | 9b2bec7092a40488108543f9334aab75 |

## Analysis Process: systemd-localed PID: 6746 Parent PID: 1

### General

| | |
|---|---|
| Start time: | 23:42:17 |
| Start date: | 01/11/2021 |
| Path: | /lib/systemd/systemd-localed |
| Arguments: | /lib/systemd/systemd-localed |
| File size: | 43232 bytes |
| MD5 hash: | 1244af9646256d49594f2a8203329aa9 |