ID: 551806
Sample Name: qFl1WpWBiv
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 15:18:14
Date: 12/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

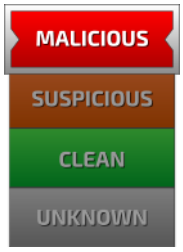
Linux Analysis Report qFl1WpWBiv

Overview

General Information

Sample Name:	qFl1WpWBiv
Analysis ID:	551806
MD5:	ed7f32a9c5ea7ce..
SHA1:	cfc52e93fcb6aef…
SHA256:	047eb2ca77f1c4f..
Tags:	32 arm elf mirai
Infos:	

Detection

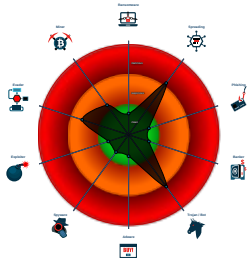


Score:	64
Range:	0 - 100
Whitelisted:	false

Signatures

- Multi AV Scanner detection for subm…
- Reads system files that contain reco…
- Sample tries to kill multiple processe…
- Sample reads /proc/mounts (often u…
- Sets full permissions to files and/or …
- Reads CPU information from /sys in…
- Executes the "mkdir" command use…
- Executes the "grep" command used…
- Uses the "uname" system call to qu…
- Executes the "chmod" command us…
- Enumerates processes within the "p…
- Sample listens on a socket

Classification



Analysis Advice

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

Non-zero exit code suggests an error during the execution. Lookup the error code for hints.

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:	551806
Start date:	12.01.2022
Start time:	15:18:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	qFl1WpWBiv
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:	mal64.spre.troj.lin@0/53@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- qFl1WpWBiv (PID: 5211, Parent: 5107, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/qFl1WpWBiv
  - qFl1WpWBiv New Fork (PID: 5213, Parent: 5211)
    - qFl1WpWBiv New Fork (PID: 5215, Parent: 5213)
      - qFl1WpWBiv New Fork (PID: 5217, Parent: 5215)
      - sh (PID: 5217, Parent: 5215, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "mkdir /psl1jjs2d3/ && >/psl1jjs2d3/psl1jjs2d3 && cd /psl1jjs2d3/ >/dev/null"

- sh New Fork (PID: 5219, Parent: 5217)
  - mkdir (PID: 5219, Parent: 5217, MD5: 088c9d1df5a28ed16c726eca15964cb7) Arguments: mkdir /psl1jjs2d3/
- qFl1WpWBiv New Fork (PID: 5220, Parent: 5215)
- sh (PID: 5220, Parent: 5215, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -c "mv /tmp/qFl1WpWBiv /psl1jjs2d3/psl1jjs2d3 && chmod 777 /psl1jjs2d3/psl1jjs2d3 >/dev/null"
  - sh New Fork (PID: 5222, Parent: 5220)
  - mv (PID: 5222, Parent: 5220, MD5: 504f0590fa482d4da070a702260e3716) Arguments: mv /tmp/qFl1WpWBiv /psl1jjs2d3/psl1jjs2d3
  - sh New Fork (PID: 5223, Parent: 5220)
  - chmod (PID: 5223, Parent: 5220, MD5: 739483b900c045ae1374d6f53a86a279) Arguments: chmod 777 /psl1jjs2d3/psl1jjs2d3
- qFl1WpWBiv New Fork (PID: 5224, Parent: 5215)
- qFl1WpWBiv New Fork (PID: 5226, Parent: 5215)
- qFl1WpWBiv New Fork (PID: 5227, Parent: 5215)
  - qFl1WpWBiv New Fork (PID: 5381, Parent: 5227)

- dash New Fork (PID: 5240, Parent: 4331)
- cat (PID: 5240, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.cKEJqxaxsv
- dash New Fork (PID: 5241, Parent: 4331)
- head (PID: 5241, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5242, Parent: 4331)
- tr (PID: 5242, Parent: 4331, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5243, Parent: 4331)
- cut (PID: 5243, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5244, Parent: 4331)
- cat (PID: 5244, Parent: 4331, MD5: 7e9d213e404ad3bb82e4ebb2e1f2c1b3) Arguments: cat /tmp/tmp.cKEJqxaxsv
- dash New Fork (PID: 5245, Parent: 4331)
- head (PID: 5245, Parent: 4331, MD5: fd96a67145172477dd57131396fc9608) Arguments: head -n 10
- dash New Fork (PID: 5246, Parent: 4331)
- tr (PID: 5246, Parent: 4331, MD5: fbd1402dd9f72d8ebfff00ce7c3a7bb5) Arguments: tr -d \\000-\\011\\013\\014\\016-\\037
- dash New Fork (PID: 5247, Parent: 4331)
- cut (PID: 5247, Parent: 4331, MD5: d8ed0ea8f22c0de0f8692d4d9f1759d3) Arguments: cut -c -80
- dash New Fork (PID: 5248, Parent: 4331)
- rm (PID: 5248, Parent: 4331, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.cKEJqxaxsv /tmp/tmp.o57W8c2jCH /tmp/tmp.9D8VQf5YAB
- systemd New Fork (PID: 5283, Parent: 1)
- rsyslogd (PID: 5283, Parent: 1, MD5: 0b8087fc907c42eb3c81a691db258e33) Arguments: /usr/sbin/rsyslogd -n -iNONE
- systemd New Fork (PID: 5308, Parent: 1)
- whoopsie (PID: 5308, Parent: 1, MD5: d3a6915d0e7398fb4c89a037c13959c8) Arguments: /usr/bin/whoopsie -f
- gdm3 New Fork (PID: 5319, Parent: 1320)
- Default (PID: 5319, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5338, Parent: 1320)
- Default (PID: 5338, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5346, Parent: 1860)
- pulseaudio (PID: 5346, Parent: 1860, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5352, Parent: 1)
- accounts-daemon (PID: 5352, Parent: 1, MD5: 01a899e3fb5e7e434bea1290255a1f30) Arguments: /usr/lib/accountsservice/accounts-daemon
  - accounts-daemon New Fork (PID: 5367, Parent: 5352)
  - language-validate (PID: 5367, Parent: 5352, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/share/language-tools/language-validate en_US.UTF-8
    - language-validate New Fork (PID: 5368, Parent: 5367)
    - language-options (PID: 5368, Parent: 5367, MD5: 16a21f464119ea7fad1d3660de963637) Arguments: /usr/share/language-tools/language-options
      - language-options New Fork (PID: 5369, Parent: 5368)
      - sh (PID: 5369, Parent: 5368, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: sh -c "locale -a | grep -F .utf8 "
        - sh New Fork (PID: 5370, Parent: 5369)
        - locale (PID: 5370, Parent: 5369, MD5: c72a78792469db86d91369c9057f20d2) Arguments: locale -a
        - sh New Fork (PID: 5371, Parent: 5369)
        - grep (PID: 5371, Parent: 5369, MD5: 1e6ebb9dd094f774478f72727bdba0f5) Arguments: grep -F .utf8
- gdm-session-worker New Fork (PID: 5363, Parent: 1809)
- Default (PID: 5363, Parent: 1809, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PostSession/Default
- gdm3 New Fork (PID: 5374, Parent: 1320)
- gdm-session-worker (PID: 5374, Parent: 1320, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
  - gdm-session-worker New Fork (PID: 5385, Parent: 5374)
  - gdm-wayland-session (PID: 5385, Parent: 5374, 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: 5388, Parent: 5385)
    - dbus-run-session (PID: 5388, Parent: 5385, MD5: 245f3ef6a268850b33b0225a8753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
      - dbus-run-session New Fork (PID: 5389, Parent: 5388)
      - dbus-daemon (PID: 5389, Parent: 5388, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --nofork --print-address 4 --session
        - dbus-daemon New Fork (PID: 5416, Parent: 5389)
          - dbus-daemon New Fork (PID: 5417, Parent: 5416)
          - false (PID: 5417, Parent: 5416, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5419, Parent: 5389)
          - dbus-daemon New Fork (PID: 5420, Parent: 5419)
          - false (PID: 5420, Parent: 5419, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5421, Parent: 5389)
          - dbus-daemon New Fork (PID: 5422, Parent: 5421)
          - false (PID: 5422, Parent: 5421, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5426, Parent: 5389)
          - dbus-daemon New Fork (PID: 5427, Parent: 5426)
          - false (PID: 5427, Parent: 5426, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5428, Parent: 5389)
          - dbus-daemon New Fork (PID: 5429, Parent: 5428)
          - false (PID: 5429, Parent: 5428, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5430, Parent: 5389)
          - dbus-daemon New Fork (PID: 5431, Parent: 5430)
          - false (PID: 5431, Parent: 5430, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5433, Parent: 5389)
          - dbus-daemon New Fork (PID: 5434, Parent: 5433)
          - false (PID: 5434, Parent: 5433, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
      - dbus-run-session New Fork (PID: 5391, Parent: 5388)
      - gnome-session (PID: 5391, Parent: 5388, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: gnome-session --autostart /usr/share/gdm/greeter/autostart
      - gnome-session-binary (PID: 5391, Parent: 5388, MD5: d9b90be4f7db60cb3c2d3da6a1d31bfb) Arguments: /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart

- gnome-session-binary New Fork (PID: 5435, Parent: 5391)
- session-migration (PID: 5435, Parent: 5391, MD5: 5227af42ebf14ac2fe2acddb002f68dc) Arguments: session-migration
- gnome-session-binary New Fork (PID: 5438, Parent: 5391)
- sh (PID: 5438, Parent: 5391, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell
- gnome-shell (PID: 5438, Parent: 5391, MD5: da7a257239677622fe4b3a65972c9e87) Arguments: /usr/bin/gnome-shell

- gdm3 New Fork (PID: 5377, Parent: 1320)
- Default (PID: 5377, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gvfsd-fuse New Fork (PID: 5396, Parent: 2038)
- fusermount (PID: 5396, Parent: 2038, MD5: 576a1b135c82bdcbc97a91acea900566) Arguments: fusermount -u -q -z -- /run/user/1000/gvfs
- systemd New Fork (PID: 5407, Parent: 1)
- systemd-user-runtime-dir (PID: 5407, Parent: 1, MD5: d55f4b0847f88131dbcfb07435178e54) Arguments: /lib/systemd/systemd-user-runtime-dir stop 1000
- gdm3 New Fork (PID: 5461, Parent: 1320)
- gdm-session-worker (PID: 5461, Parent: 1320, MD5: 692243754bd9f38fe9bd7e230b5c060a) Arguments: "gdm-session-worker [pam/gdm-launch-environment]"
  - gdm-session-worker New Fork (PID: 5469, Parent: 5461)
  - gdm-x-session (PID: 5469, Parent: 5461, 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: 5471, Parent: 5469)
    - Xorg (PID: 5471, Parent: 5469, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /usr/bin/Xorg vt1 -displayfd 3 -auth /run/user/127/gdm/Xauthority -background none -noreset -keeptty -verbose 3
    - Xorg.wrap (PID: 5471, Parent: 5469, 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: 5471, Parent: 5469, 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: 5480, Parent: 5471)
      - sh (PID: 5480, Parent: 5471, 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: 5481, Parent: 5480)
        - xkbcomp (PID: 5481, Parent: 5480, 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: 5715, Parent: 5471)
      - sh (PID: 5715, Parent: 5471, 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: 5716, Parent: 5715)
        - xkbcomp (PID: 5716, Parent: 5715, 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: 5487, Parent: 5469)
    - Default (PID: 5487, Parent: 5469, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/Prime/Default
    - gdm-x-session New Fork (PID: 5488, Parent: 5469)
    - dbus-run-session (PID: 5488, Parent: 5469, MD5: 245f3ef6a268850b33b0225a8753b7f4) Arguments: dbus-run-session -- gnome-session --autostart /usr/share/gdm/greeter/autostart
      - dbus-run-session New Fork (PID: 5489, Parent: 5488)
      - dbus-daemon (PID: 5489, Parent: 5488, MD5: 3089d47e3f3ab84cd81c48fd406d7a8c) Arguments: dbus-daemon --nofork --print-address 4 --session
        - dbus-daemon New Fork (PID: 5505, Parent: 5489)
          - dbus-daemon New Fork (PID: 5506, Parent: 5505)
          - at-spi-bus-launcher (PID: 5506, Parent: 5505, MD5: 1563f274acd4e7ba530a55bdc4c95682) Arguments: /usr/libexec/at-spi-bus-launcher
            - at-spi-bus-launcher New Fork (PID: 5511, Parent: 5506)
            - dbus-daemon (PID: 5511, Parent: 5506, 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: 5830, Parent: 5511)
                - dbus-daemon New Fork (PID: 5831, Parent: 5830)
                - at-spi2-registryd (PID: 5831, Parent: 5830, MD5: 1d904c2693452edebc7ede3a9e24d440) Arguments: /usr/libexec/at-spi2-registryd --use-gnome-session
        - dbus-daemon New Fork (PID: 5535, Parent: 5489)
          - dbus-daemon New Fork (PID: 5536, Parent: 5535)
          - false (PID: 5536, Parent: 5535, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5538, Parent: 5489)
          - dbus-daemon New Fork (PID: 5539, Parent: 5538)
          - false (PID: 5539, Parent: 5538, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5540, Parent: 5489)
          - dbus-daemon New Fork (PID: 5541, Parent: 5540)
          - false (PID: 5541, Parent: 5540, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5542, Parent: 5489)
          - dbus-daemon New Fork (PID: 5543, Parent: 5542)
          - false (PID: 5543, Parent: 5542, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5544, Parent: 5489)
          - dbus-daemon New Fork (PID: 5545, Parent: 5544)
          - false (PID: 5545, Parent: 5544, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5546, Parent: 5489)
          - dbus-daemon New Fork (PID: 5547, Parent: 5546)
          - false (PID: 5547, Parent: 5546, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5549, Parent: 5489)
          - dbus-daemon New Fork (PID: 5550, Parent: 5549)
          - false (PID: 5550, Parent: 5549, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
        - dbus-daemon New Fork (PID: 5713, Parent: 5489)
          - dbus-daemon New Fork (PID: 5714, Parent: 5713)
          - ibus-portal (PID: 5714, Parent: 5713, MD5: 562ad55bd9a4d54bd7b76746b01e37d3) Arguments: /usr/libexec/ibus-portal
        - dbus-daemon New Fork (PID: 5833, Parent: 5489)
          - dbus-daemon New Fork (PID: 5834, Parent: 5833)
          - gjs (PID: 5834, Parent: 5833, MD5: 5f3eceb792bb65c22f23d1efb4fde3ad) Arguments: /usr/bin/gjs /usr/share/gnome-shell/org.gnome.Shell.Notifications
        - dbus-daemon New Fork (PID: 5899, Parent: 5489)
          - dbus-daemon New Fork (PID: 5900, Parent: 5899)
          - false (PID: 5900, Parent: 5899, MD5: 3177546c74e4f0062909eae43d948bfc) Arguments: /bin/false
      - dbus-run-session New Fork (PID: 5490, Parent: 5488)
      - gnome-session (PID: 5490, Parent: 5488, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: gnome-session --autostart /usr/share/gdm/greeter/autostart
      - gnome-session-binary (PID: 5490, Parent: 5488, MD5: d9b90be4f7db60cb3c2d3da6a1d31bfb) Arguments: /usr/libexec/gnome-session-binary --systemd --autostart /usr/share/gdm/greeter/autostart
        - gnome-session-binary New Fork (PID: 5493, Parent: 5490)
        - gnome-session-check-accelerated (PID: 5493, Parent: 5490, MD5: a64839518af85b2b9de31aca27646396) Arguments: /usr/libexec/gnome-session-check-accelerated
          - gnome-session-check-accelerated New Fork (PID: 5512, Parent: 5493)

- gnome-session-check-accelerated-gl-helper (PID: 5512, Parent: 5493, MD5: b1ab9a384f9e98a39ae5c36037dd5e78) Arguments: /usr/libexec/gnome-session-check-accelerated-gl-helper --print-renderer
- gnome-session-check-accelerated New Fork (PID: 5522, Parent: 5493)
- gnome-session-check-accelerated-gles-helper (PID: 5522, Parent: 5493, MD5: 1bd78885765a18e60c05ed1fb5fa3bf8) Arguments: /usr/libexec/gnome-session-check-accelerated-gles-helper --print-renderer

- gnome-session-binary New Fork (PID: 5551, Parent: 5490)
- session-migration (PID: 5551, Parent: 5490, MD5: 5227af42ebf14ac2fe2acddb002f68dc) Arguments: session-migration
- gnome-session-binary New Fork (PID: 5552, Parent: 5490)
- sh (PID: 5552, Parent: 5490, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/gnome-shell
- gnome-shell (PID: 5552, Parent: 5490, MD5: da7a257239677622fe4b3a65972c9e87) Arguments: /usr/bin/gnome-shell
  - gnome-shell New Fork (PID: 5588, Parent: 5552)
  - ibus-daemon (PID: 5588, Parent: 5552, MD5: 1e00fb9860b198c73f6e364e3ff16f31) Arguments: ibus-daemon --panel disable --xim
    - ibus-daemon New Fork (PID: 5708, Parent: 5588)
    - ibus-memconf (PID: 5708, Parent: 5588, MD5: 523e939905910d06598e66385761a822) Arguments: /usr/libexec/ibus-memconf
    - ibus-daemon New Fork (PID: 5711, Parent: 5588)
      - ibus-daemon New Fork (PID: 5712, Parent: 5711)
      - ibus-x11 (PID: 5712, Parent: 1, MD5: 2aa1e54666191243814c2733d6992dbd) Arguments: /usr/libexec/ibus-x11 --kill-daemon
    - ibus-daemon New Fork (PID: 5873, Parent: 5588)
    - ibus-engine-simple (PID: 5873, Parent: 5588, MD5: 0238866d5e8802a0ce1b1b9af8cb1376) Arguments: /usr/libexec/ibus-engine-simple
- gnome-session-binary New Fork (PID: 5854, Parent: 5490)
- sh (PID: 5854, Parent: 5490, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sharing
- gsd-sharing (PID: 5854, Parent: 5490, MD5: e29d9025d98590fbb69f89fdbd4438b3) Arguments: /usr/libexec/gsd-sharing
- gnome-session-binary New Fork (PID: 5856, Parent: 5490)
- sh (PID: 5856, Parent: 5490, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-wacom
- gsd-wacom (PID: 5856, Parent: 5490, MD5: 13778dd1a23a4e94ddc17ac9caa4fcc1) Arguments: /usr/libexec/gsd-wacom
- gnome-session-binary New Fork (PID: 5858, Parent: 5490)
- sh (PID: 5858, Parent: 5490, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-color
- gsd-color (PID: 5858, Parent: 5490, MD5: ac2861ad93ce047283e8e87cefef9a19) Arguments: /usr/libexec/gsd-color
- gnome-session-binary New Fork (PID: 5859, Parent: 5490)
- sh (PID: 5859, Parent: 5490, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-keyboard
- gsd-keyboard (PID: 5859, Parent: 5490, MD5: 8e288fd17c80bb0a1148b964b2ac2279) Arguments: /usr/libexec/gsd-keyboard
- gnome-session-binary New Fork (PID: 5860, Parent: 5490)
- sh (PID: 5860, Parent: 5490, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-print-notifications
- gsd-print-notifications (PID: 5860, Parent: 5490, MD5: 71539698aa691718cee775d6b9450ae2) Arguments: /usr/libexec/gsd-print-notifications
  - gsd-print-notifications New Fork (PID: 6032, Parent: 5860)
    - gsd-print-notifications New Fork (PID: 6033, Parent: 6032)
    - gsd-printer (PID: 6033, Parent: 1, MD5: 7995828cf98c315fd55f2ffb3b22384d) Arguments: /usr/libexec/gsd-printer
- gnome-session-binary New Fork (PID: 5861, Parent: 5490)
- sh (PID: 5861, Parent: 5490, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-rfkill
- gsd-rfkill (PID: 5861, Parent: 5490, MD5: 88a16a3c0aba1759358c06215ecfb5cc) Arguments: /usr/libexec/gsd-rfkill
- gnome-session-binary New Fork (PID: 5863, Parent: 5490)
- sh (PID: 5863, Parent: 5490, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-smartcard
- gsd-smartcard (PID: 5863, Parent: 5490, MD5: ea1fbd7f62e4cd0331eae2ef754ee605) Arguments: /usr/libexec/gsd-smartcard
- gnome-session-binary New Fork (PID: 5864, Parent: 5490)
- sh (PID: 5864, Parent: 5490, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-datetime
- gsd-datetime (PID: 5864, Parent: 5490, MD5: d80d39745740de37d6634d36e344d4bc) Arguments: /usr/libexec/gsd-datetime
- gnome-session-binary New Fork (PID: 5866, Parent: 5490)
- sh (PID: 5866, Parent: 5490, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-media-keys
- gsd-media-keys (PID: 5866, Parent: 5490, MD5: a425448c135afb4b8bfd79cc0b6b74da) Arguments: /usr/libexec/gsd-media-keys
- gnome-session-binary New Fork (PID: 5867, Parent: 5490)
- sh (PID: 5867, Parent: 5490, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-screensaver-proxy
- gsd-screensaver-proxy (PID: 5867, Parent: 5490, MD5: 77e309450c87dceee43f1a9e50cc0d02) Arguments: /usr/libexec/gsd-screensaver-proxy
- gnome-session-binary New Fork (PID: 5868, Parent: 5490)
- sh (PID: 5868, Parent: 5490, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-sound
- gsd-sound (PID: 5868, Parent: 5490, MD5: 4c7d3fb993463337b4a0eb5c80c760ee) Arguments: /usr/libexec/gsd-sound
- gnome-session-binary New Fork (PID: 5872, Parent: 5490)
- sh (PID: 5872, Parent: 5490, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-a11y-settings
- gsd-a11y-settings (PID: 5872, Parent: 5490, MD5: 18e243d2cf30ecee7ea89d1462725c5c) Arguments: /usr/libexec/gsd-a11y-settings
- gnome-session-binary New Fork (PID: 5875, Parent: 5490)
- sh (PID: 5875, Parent: 5490, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-housekeeping
- gsd-housekeeping (PID: 5875, Parent: 5490, MD5: b55f3394a84976ddb92a2915e5d76914) Arguments: /usr/libexec/gsd-housekeeping
- gnome-session-binary New Fork (PID: 5880, Parent: 5490)
- sh (PID: 5880, Parent: 5490, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/libexec/gsd-power
- gsd-power (PID: 5880, Parent: 5490, MD5: 28b8e1b43c3e7f1db6741ea1ecd978b7) Arguments: /usr/libexec/gsd-power
- gnome-session-binary New Fork (PID: 6335, Parent: 5490)
- sh (PID: 6335, Parent: 5490, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh /usr/bin/spice-vdagent
- spice-vdagent (PID: 6335, Parent: 5490, MD5: 80fb7f613aa78d1b8a229dbcf4577a9d) Arguments: /usr/bin/spice-vdagent
- gnome-session-binary New Fork (PID: 6340, Parent: 5490)
- sh (PID: 6340, Parent: 5490, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /bin/sh -e -u -c "export GIO_LAUNCHED_DESKTOP_FILE_PID=$$; exec \"$@\"" sh xbrlapi -q
- xbrlapi (PID: 6340, Parent: 5490, MD5: 0cfe25df39d38af32d6265ed947ca5b9) Arguments: xbrlapi -q

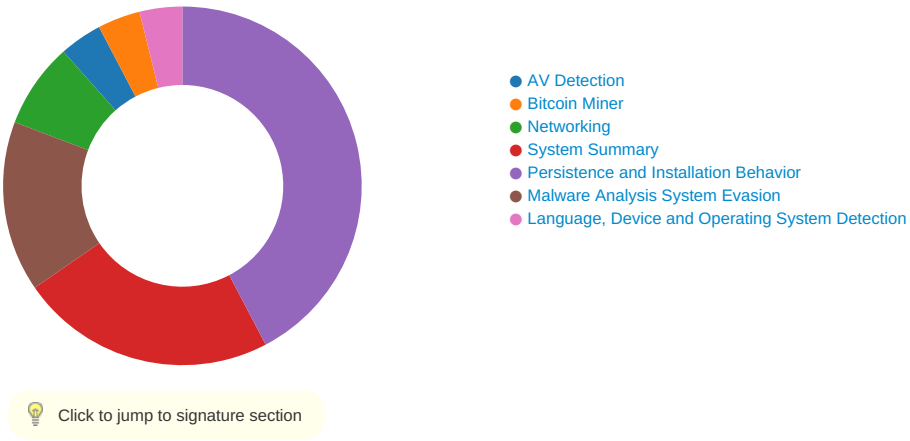
- gdm3 New Fork (PID: 5462, Parent: 1320)
- Default (PID: 5462, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- gdm3 New Fork (PID: 5463, Parent: 1320)

- Default (PID: 5463, Parent: 1320, MD5: 1e6b1c887c59a315edb7eb9a315fc84c) Arguments: /etc/gdm3/PrimeOff/Default
- systemd New Fork (PID: 5577, Parent: 1)
- systemd-localed (PID: 5577, Parent: 1, MD5: 1244af9646256d49594f2a8203329aa9) Arguments: /lib/systemd/systemd-localed
- systemd New Fork (PID: 5724, Parent: 1334)
- pulseaudio (PID: 5724, Parent: 1334, MD5: 0c3b4c789d8ffb12b25507f27e14c186) Arguments: /usr/bin/pulseaudio --daemonize=no --log-target=journal
- systemd New Fork (PID: 5725, Parent: 1)
- geoclue (PID: 5725, Parent: 1, MD5: 30ac5455f3c598dde91dc87477fb19f7) Arguments: /usr/libexec/geoclue
- systemd New Fork (PID: 5901, Parent: 1)
- systemd-hostnamed (PID: 5901, Parent: 1, MD5: 2cc8a5576629a2d5bd98e49a4b8bef65) Arguments: /lib/systemd/systemd-hostnamed
- systemd New Fork (PID: 6076, Parent: 1)
- fprintd (PID: 6076, Parent: 1, MD5: b0d8829f05cd028529b84b061b660e84) Arguments: /usr/libexec/fprintd
- systemd New Fork (PID: 6201, Parent: 1)
- systemd-localed (PID: 6201, Parent: 1, MD5: 1244af9646256d49594f2a8203329aa9) Arguments: /lib/systemd/systemd-localed
- **cleanup**

Yara Overview

No yara matches

Jbx Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

System Summary:

Sample tries to kill multiple processes (SIGKILL)

Persistence and Installation Behavior:

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

Sets full permissions to files and/or directories

Language, Device and Operating System Detection:

Reads system files that contain records of logged in users

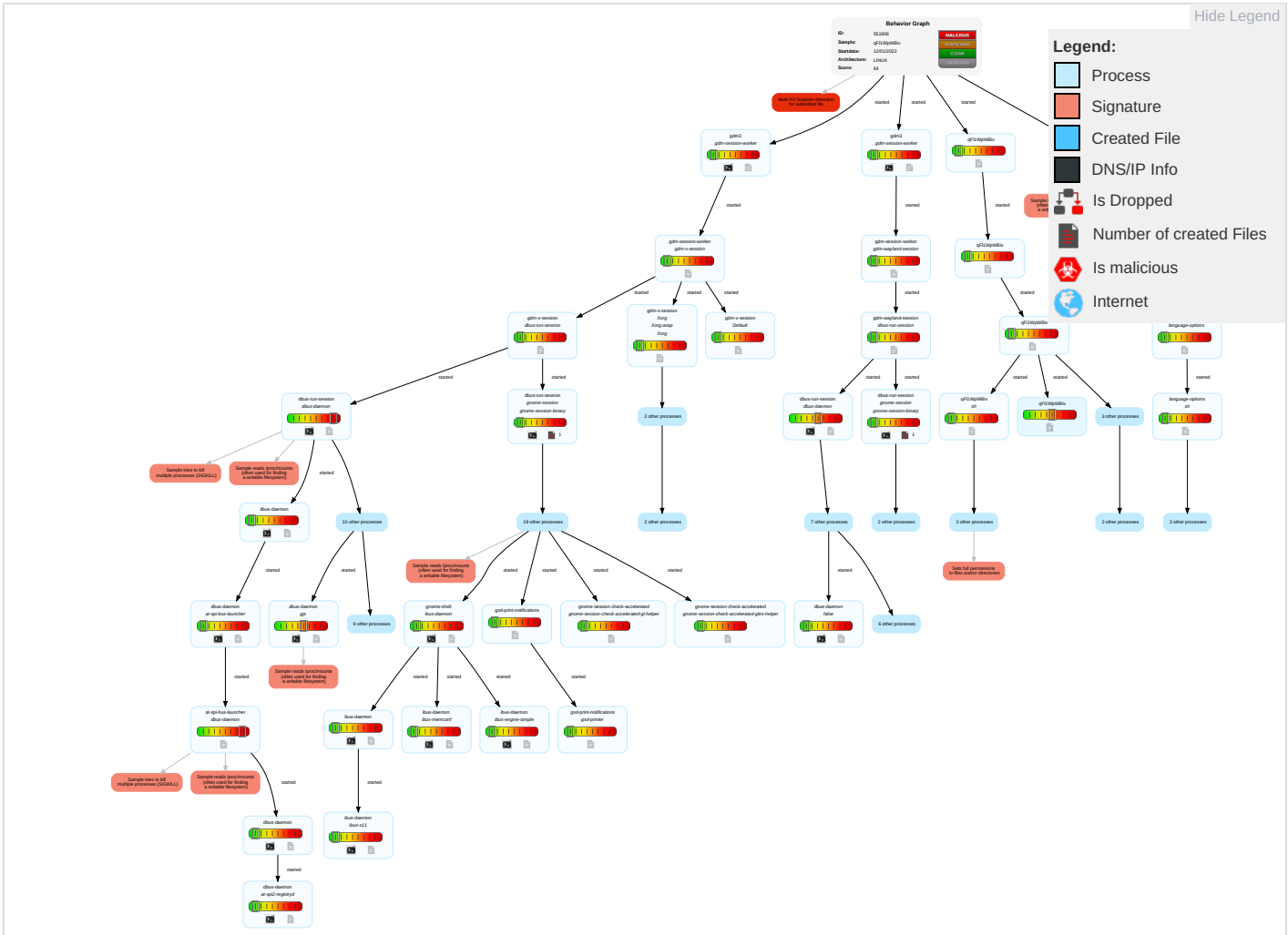
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	In
Valid Accounts	Command and Scripting Interpreter 1	Path Interception	Path Interception	File and Directory Permissions Modification 2	OS Credential Dumping 1	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M Sy Pa
Default Accounts	Scripting 1	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	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D Lo
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	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D Da
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Indicator Removal on Host 1	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		C Bi Fr
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		M Ap Ra or

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
qFl1WpWBiv	33%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://%d.%d.%d.%d:%d/%s	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

Runtime Messages

Command:	/tmp/qFl1WpWBiv
Exit Code:	1
Exit Code Info:	
Killed:	False
Standard Output:	
Standard Error:	

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

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
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:	3:5bkrIZsXvn:pkckv
MD5:	28FE6435F34B3367707BB1C5D5F6B430
SHA1:	EB8FE2D16BD6BBCCE106C94E4D284543B2573CF6
SHA-256:	721A37C69E555799B41D308849E8F8125441883AB021B723FED90A9B744F36C0
SHA-512:	6B6AB7C0979629D0FEF6BE47C5C6BCC367EDD0AAE3FC973F4DE2FD5F0A819C89E7656DB65D453B1B5398E54012B27EDFE02894AD87A7E0AF3A9C5F2EB24A919
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	auto_null.monitor.

/proc/5417/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/5420/oom_score_adj	
Process:	/usr/bin/dbus-daemon
File Type:	very short file (no magic)

/proc/5420/oom_score_adj	
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 99
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	 0

/proc/5422/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 99
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	 0

/proc/5427/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 99
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	 0

/proc/5429/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 99
Malicious:	false
Preview:	 0

/proc/5431/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 99
Malicious:	false
Preview:	 0

/proc/5434/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 99
Malicious:	false
Preview:	 0

/proc/5506/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 99
Malicious:	false
Preview:	 0

/proc/5536/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 99
Malicious:	false
Preview:	 0

/proc/5539/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 99
Malicious:	false
Preview:	 0

/proc/5541/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 99
Malicious:	false
Preview:	 0

/proc/5543/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 99
Malicious:	false
Preview:	 0

/proc/5545/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 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 99
Malicious:	false
Preview:	 0

/proc/5550/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 99
Malicious:	false
Preview:	 0

/proc/5714/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 99
Malicious:	false
Preview:	 0

/proc/5831/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 99
Malicious:	false
Preview:	 0

/proc/5834/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 99
Malicious:	false
Preview:	 0

/proc/5900/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 99
Malicious:	false
Preview:	 0

/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:DRTvn:NTvn
MD5:	EDB88945C12733FA78789860D73FF367
SHA1:	0F21490844802E32624F158BD37DD20744E3A316
SHA-256:	40018B450E07A9E38210DDAFAB88184450EC579EF6F51500FD08275F0A42EF83
SHA-512:	230012C0C1BEA78D5D61CA6A9BBEF91303C7B7543834EB3D96F9C93841F57DBABB2EA83DA492F7B362BEE2690EE705EB17763D4A49E91BE6C26B3A03E2D7E9 47
Malicious:	false
Preview:	 5346.

/run/user/127/ICEauthority	
Process:	/usr/libexec/gnome-session-binary
File Type:	data
Category:	dropped
Size (bytes):	1304
Entropy (8bit):	6.014406895508527
Encrypted:	false
SSDEEP:	12:OxP8L/ROveY+80G83xPY3ZveY+Y3QO4gxP5mhijveY+5tWmxPwWoveY+wcZVveY8:r/3zOvDfwqrIBtZ+
MD5:	85FAAD43F438A3EFF5C2557B704FA11B
SHA1:	9652025675FBB0980DDBFB109617E00F9891A299
SHA-256:	3CAAD84539FCCC70158754D4ACC6B383B775C7FBB4C23B5FA5222E1922455AD5
SHA-512:	B00576CB0DEDC646795CB395DA103DECB47A15D71D99C1505E0DD9E554803983A2F1D9A121409090A8FC3806730AD96AF375DAE59247BC464D3CDDC8B30303 A
Malicious:	false

/run/user/127/ICEauthority	
Preview:	..XSMP...!unix/galassia:/tmp/.ICE-unix/5490..MIT-MAGIC-COOKIE-1..{q.4..>|.4.a5.....XSMP...#local/galassia:@/tmp/.ICE-unix/5490..MIT-MAGIC-COOKIE-1..b....K..1n.. .b.t..ICE...!unix/galassia:/tmp/.ICE-unix/5391..MIT-MAGIC-COOKIE-1.....2.....[/.<..ICE...#local/galassia:@/tmp/.ICE-unix/5391..MIT-MAGIC-COOKIE-1.....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...}.9...ICE...!un ix/galassia:/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...w$....^.'fl..1..ICE...#local/galassia:@/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...^f.....E..c..XSMP...#l ocal/galassia:@/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1... .....Y...@.t...XSMP...!unix/galassia:/tmp/.ICE-unix/1348..MIT-MAGIC-COOKIE-1...#...,.:B.o.....ICE... #local/galassia:@/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1..N..yte\|4yXJ...Mf..ICE...!unix/galassia:/tmp/.ICE-unix/1477..MIT-MAGIC-COOKIE-1.....cN.....N+..$..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):	4.882427239163554
Encrypted:	false
SSDEEP:	3:rg/WFllasO93QBnjBahgWFllasO93QBnjBn:rg/WFl2yn9zWFl2yn9n
MD5:	4CC786AF03C7E1A518724525E9322966
SHA1:	4276B2EC05292EE91203F75C3684CAFFD01F8080
SHA-256:	6274E1389ECCC76921D285A8D0C4ECC25ACF2D4B4AC111FE644636FE5FA7721D
SHA-512:	51D6E369F3457B499A3DC3B1E43E980999316CF0BCFA9201208357578098815978D3EA47783F6FFA96C57D8B643AE9E8C7E728D9A73D9D70F867EA247113D1A1
Malicious:	false
Preview:	....galassia....MIT-MAGIC-COOKIE-1..b..71..E..#V<a:....galassia....MIT-MAGIC-COOKIE-1..b..71..E..#V<a:

/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:HXJ:3J
MD5:	677B2EDA9B18B7C1E2FAA04FD2337B52
SHA1:	16DABFBE65CE93E0454DC2096AC511B5D08C684B
SHA-256:	67500AE174639BB135B2C888C60744AC2FEFB5C07F2813CE224BC90FAE39315C
SHA-512:	23C1902274EBB84C4370192949FAFC5ADF89CB1AE458F653A67E0C52333B45385BEE68E360179DA58FACD397AEE4CAB72EF9E1E516C606666B40D2C084C40B5F
Malicious:	false
Preview:	5724.

/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
Encrypted:	false
SSDEEP:	192:tDyb2zOmnECQmwTVFfLaSLus4UVcqLkjoqdD//HJeCQ1+JdDx0s2T:tDyAxvYhFf+S6tUzmp7/1MJ
MD5:	B4E3EB0B8B6B0FC1F46740C573E18D86
SHA1:	7D35426357695EBA77850757E8939A62DCEFF2D1

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

/var/cache/motd-news	
Process:	/usr/bin/cut
File Type:	ASCII text
Category:	dropped
Size (bytes):	191
Entropy (8bit):	4.515771857099866
Encrypted:	false
SSDEEP:	3:P2lnI+5MsqqzNLz+FRNScHUBfRau95++sZzR5woLB1Fh0VTGTl/X5kURn:OZ8uNLzDc0pR75+9Zz/woFmIT52URn
MD5:	DD514F892B5F93ED615D366E58AC58AF
SHA1:	BA75EDB3C2232CC260BC187F604DC8F25AA72C11
SHA-256:	F40D0DCE6E83DF74109FEF5E68E51CC255727783EEAE04C3E34677E23F7552CF
SHA-512:	9150BDE63F6C4850C5340D8877892B4D9BBF9EBDC98CDCF557A93FA304C1222CEE446418F5BE2ACCDBF38393778AFA5D4F3EDCB37A47BF57D3A4B2DEAD42A 2D0
Malicious:	false
Preview:	* Super-optimized for small spaces - read how we shrank the memory. footprint of MicroK8s to make it the smallest full K8s around... https://ubuntu.com/blog/microk8s-memory-optimisation.

/var/lib/AccountsService/users/gdm.6UMQF1	
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 AEA
Malicious:	false
Preview:	[User].XSession=.Icon=/var/lib/gdm3/.face.SystemAccount=true.

/var/lib/AccountsService/users/gdm.RA0MF1	
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 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

/var/lib/gdm3/.config/ibus/bus/ee49dfd4fa47433baee88884e2d7de7c-unix-0	
Category:	dropped
Size (bytes):	381
Entropy (8bit):	5.202707668054676
Encrypted:	false
SSDEEP:	6:SbF4b2sONeZVkSoQ65EfqFFAU+qmnQT23msRvkTFacecf8h/zKLGWWMztTp19dv:q5sU3LWfLUDmQymqSFbfomSA9ft
MD5:	38055F648003B260F8F109826F5A39F8
SHA1:	2FFE3ED4B993778E0F205B398695A345E5CFCACF
SHA-256:	A71E2BA8FB4454948CAF6035E77FC247F178D2CAE72FCB79C181F69DE358F6BD
SHA-512:	E635A441F1692729E4E12EB94D656572A48128536F9CAA223630FB896F0665789DE067BE6FB5A416E3D00257AE2DA4BFBB2E3502FF57C373B73C189C8B64D8FC
Malicious:	false
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-1XN5TqCL,guid=e8224159d6629ac334c7799061def203.IBUS_DAEMON_PID=5588.

/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/lib/whoopsie/whoopsie-id.Y35LF1	
Process:	/usr/bin/whoopsie
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	128
Entropy (8bit):	3.9410969045919657
Encrypted:	false
SSDEEP:	3:19y6UTAvBTdDVEQcNgAT0XUQhd3tjCZccCKcsVQWQ7JW:3y6BlVEfQXU8djCZd40
MD5:	D2B5AAF22916F8D6665CF9E835EAD5E7
SHA1:	AAEF3CE527B8F1E3733BCD03EF7A6C0F30881E15
SHA-256:	FEB925D4465BF6D30A42B19112406AD1B59BA90673DC4F91B25005A90FEFEB36
SHA-512:	B55A45FA0DECE5A3B0348BC3F3031A7329590E57BAD5013690AFEAA9825C0DE4B75D27057A56C33800F1626935840DA2262AAF14E795C75F39362B728D95F18A
Malicious:	false
Preview:	9aadafe2051348cd32033e1cad68f0a5fe46fba3240ac1e6e42158f31b8a1371790c09baf3996b4979fe8e533446c7dedf30f654c68b25357334c66911dc6a9e

/var/log/Xorg.0.log	
Process:	/usr/lib/xorg/Xorg

/var/log/Xorg.0.log	
File Type:	ASCII text
Category:	dropped
Size (bytes):	41347
Entropy (8bit):	5.293189412035658
Encrypted:	false
SSDEEP:	384:rmjk5YSyDHpGMedDdHdnd7dqdGdHdOdAd2d4dKdIdLd3dud5d+dBdkdJEdkndHqq:CjkVyDH7F86/m32G7povmjAkjPfO
MD5:	3D4982D31B8C77709943A4DED12D2B7B
SHA1:	848F7E5D8105F725DD1F545E163B3ED853C84AA5
SHA-256:	F82A4A7092FA160C868FFF41BDDAC1051D17AA5BAF2C8B71300B4872A6F3C43C
SHA-512:	D74D260D9E66184A2AF4EE91B9CE11AC9FCD9243B6339ACAA18DB0C503A5E729126868BEF6A89D8860DF9BAB668EE3650AEE03066F09F89308D19E2B2374C19 6
Malicious:	false
Preview:	[531.128] (--) Log file renamed from "/var/log/Xorg.pid-5471.log" to "/var/log/Xorg.0.log".[531.147] .X.Org X Server 1.20.11.X Protocol Version 11, Revision 0.[5 31.157] Build Operating System: linux Ubuntu.[531.164] Current Operating System: Linux galassia 5.4.0-72-generic #80-Ubuntu SMP Mon Apr 12 17:35:00 UTC 2021 x86_64.[531.171] Kernel command line: Patched by Joe: BOOT_IMAGE=/vmlinuz-5.4.0-72-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro maybe-ubiquity.[531.1 88] Build Date: 06 July 2021 10:17:51AM.[531.195] xorg-server 2:1.20.11-1ubuntu1~20.04.2 (For technical support please see http://www.ubuntu.com/support) .[531.204] Current version of pixman: 0.38.4.[531.216] .Before reporting problems, check http://wiki.x.org..to make sure that you have the latest version..[531.230] Markers: (--) probed, (**) from config file, (==) default setting,..(++) from command line, (!!) notice, (II) informational,..(WW) warning, (EE) error, (NI) not implemented, (??)

/var/log/auth.log	
Process:	/usr/sbin/rsyslogd
File Type:	ASCII text
Category:	dropped
Size (bytes):	2213
Entropy (8bit):	5.00475974818684
Encrypted:	false
SSDEEP:	24:ydjjuYgDwtFdAydjjHiM1A49tFdmDkMcrCQtFdAxjodcXjO3dNuKKMcrCQU:I8DcAIGM1A4rmJcrCQAxbyyKfcrCn
MD5:	32230D72F3FE575770637FB4D8B33DBA
SHA1:	1059C56FDDD780F87B1E2A2B84BB0C5A884C9763
SHA-256:	3A2EBA02529E4D24FB52EBA7343B7C9B66F77260373D11AFD7ECDF4E42478934
SHA-512:	4B1B19BA3FF98DC29836D896D0DBF660ED4DD2813E3948C3FED52D122323AFB47E339700705A901457FD5143808360BA9707562388DA6BC4862D7102B91F7FF1
Malicious:	false
Preview:	Jan 12 15:20:07 galassia polkitd(authority=local): Unregistered Authentication Agent for unix-session:c2 (system bus name :1.43, object path /org/freedesktop/PolicyKit1/A uthenticationAgent, locale en_US.UTF-8) (disconnected from bus).Jan 12 15:20:07 galassia gdm-launch-environment]: pam_unix(gdm-launch-environment:session): sess ion closed for user gdm.Jan 12 15:20:07 galassia systemd-logind[797]: Session c2 logged out. Waiting for processes to exit..Jan 12 15:20:07 galassia systemd-log ind[797]: Removed session c2..Jan 12 15:20:27 galassia polkitd(authority=local): Unregistered Authentication Agent for unix-session:2 (system bus name :1.87, object path /org/gnome/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus).Jan 12 15:20:27 galassia gdm-password]: pam_unix(gdm-password:session): s ession closed for user saturnino.Jan 12 15:20:33 galassia systemd-logind[797]: Session 2 logged out. Waiting for processes to exit..Jan 12 15:20:33 galassia systemd-logind[797]: Re

/var/log/kern.log	
Process:	/usr/sbin/rsyslogd
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	44390
Entropy (8bit):	4.8698390785711725
Encrypted:	false
SSDEEP:	384:+J+A8HHMJEG7bbPUNjyJezU1Jku5EEo7JN291GPFRyxG20KP3BaLCdHaD2UwTLYh:PMvbbMRs1Jk7
MD5:	F147A41E5FD976AD4CAFF03AA3E8289F
SHA1:	9FA0E62C0CB73DBB326C2939EF844F717D3F7097
SHA-256:	7CC3C61198460C845AC140F450418478155449B981C5CEA02F2E076B0FCD49FF
SHA-512:	CE02B2A27870C6925AEA23A3D398661B4D4748E360A2F336E54F968D0960F6D374607751E1D69F3071D736D4427031F6DEB67AE12C641D8DC79D8AB9B5DC2A6
Malicious:	false
Preview:	Jan 12 15:19:38 galassia kernel: [452.097192] blocking signal 9: 5224 -> 788.Jan 12 15:19:38 galassia kernel: [454.762742] New task spawned: old: (tgid 5283, tid 5283), new (tgid: 5283, tid: 5284).Jan 12 15:19:38 galassia kernel: [454.766547] New task spawned: old: (tgid 5283, tid 5283), new (tgid: 5283, tid: 5285).Jan 12 15:19:39 g alassia kernel: [454.769964] New task spawned: old: (tgid 5283, tid 5284), new (tgid: 5283, tid: 5286).Jan 12 15:19:40 galassia kernel: [456.294579] blocking signal 9: 5224 -> 797.Jan 12 15:19:42 galassia kernel: [457.395262] blocking signal 9: 5224 -> 799.Jan 12 15:19:45 galassia kernel: [458.790809] blocking signal 9: 5224 -> 80 0.Jan 12 15:19:46 galassia kernel: [462.019035] blocking signal 9: 5224 -> 847.Jan 12 15:19:49 galassia kernel: [463.142719] blocking signal 9: 5224 -> 884.Jan 12 15: 19:49 galassia kernel: [466.283462] New task spawned: old: (tgid 5308, tid 5308), new (tgid: 5308, tid: 5309).Jan 12 15:19:50 galassia kernel: [46

/var/log/syslog	
Process:	/usr/sbin/rsyslogd
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	167539
Entropy (8bit):	5.2119787529720245
Encrypted:	false

/var/log/syslog	
SSDEEP:	768:DNx7o4kOu45DPueCsqQFgLXZ+lhH8TVxAqEQUyX2yoZDH9s/bN3qu4QOlgAMeOVz:97BDwRT57+B1ZUL4FZIe6b
MD5:	66C497511D7B46F8E42CAB319B0979E4
SHA1:	26D599D27D52AAA5AD8D01B8C0817CE66676E4AA
SHA-256:	92B29FAF54E7F5BA1858D519EA9D1091B668C29120A27F4B997FF683208B1888
SHA-512:	3AF4C92E71473F5540C255B8631FF9856B3BFC9AD11F22F8564DB238C22F3E99E261C4D73253441255FB29872015373FC9C08542BD71EF4D1FA35D8301440AD9
Malicious:	false
Preview:	Jan 12 15:19:37 galassia systemd[1]: rsyslog.service: Main process exited, code=killed, status=9/KILL.Jan 12 15:19:37 galassia systemd[1]: rsyslog.service: Failed with result 'signal'..Jan 12 15:19:37 galassia systemd[1]: systemd-udevd.service: Got notification message from PID 5029, but reception is disabled..Jan 12 15:19:37 galassia systemd[1]: rsyslog.service: Scheduled restart job, restart counter is at 1..Jan 12 15:19:37 galassia systemd[1]: Stopped System Logging Service..Jan 12 15:19:37 galassia systemd[1]: Starting System Logging Service....Jan 12 15:19:38 galassia systemd[1]: Started System Logging Service..Jan 12 15:19:38 galassia kernel: [452.097192] blocking signal 9: 5224 -> 788.Jan 12 15:19:38 galassia kernel: [454.762742] New task spawned: old: (tgid 5283, tid 5283), new (tgid: 5283, tid: 5284).Jan 12 15:19:38 galassia kernel: [454.766547] New task spawned: old: (tgid 5283, tid 5283), new (tgid: 5283, tid: 5285).Jan 12 15:19:38 galassia rsyslogd: imuxsock: Acquired

Static File Info

General

File type:	ELF 32-bit LSB executable, ARM, EABI4 version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.167675579203324
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	qFl1WpWBiv
File size:	147136
MD5:	ed7f32a9c5ea7ced9cc9bc39ddb08b60
SHA1:	cfc52e93fcb6aefdbc953795c667244298977770
SHA256:	047eb2ca77f1c4f430e9b96d18a46438ee3c0188b9d391 db0252a0d677eae92
SHA512:	bfb840893388d59b495d0bbfe012e1243a45afaa9eb4a50 81bf26214b8acec6edb39c1f5bd25ba12dca319f27567e1 93fc243d694ed7be1ce3002b38668aef8d
SSDEEP:	3072:lC5NG5bp5h45Cq5g+5LW0QEfvowvXDGh70IcWf kiHQta8J87D8NsGT+kCa2Zu/8:wOj4lbxW0Q0PDGh76 Diwta8J87DAsG6Z
File Content Preview:	.ELF.....(.....4...@<.....4. ...(.....p.6..... ... .7...7.....7...7...7.....3.....7...7. ..7.....Q.td.....-...L..... @-.,@...0....S

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x8194
Flags:	0x4000002
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	5
Section Header Offset:	146496
Section Header Size:	40
Number of Section Headers:	16
Header String Table Index:	15

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
.init	PROGBITS	0x80d4	0xd4	0x10	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80f0	0xf0	0x1e39c	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x2648c	0x1e48c	0x10	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x264a0	0x1e4a0	0x51e8	0x0	0x2	A	0	0	8
.ARM.extab	PROGBITS	0x2b688	0x23688	0x18	0x0	0x2	A	0	0	4
.ARM.exidx	ARM_EXIDX	0x2b6a0	0x236a0	0x120	0x0	0x82	AL	2	0	4
.eh_frame	PROGBITS	0x337c0	0x237c0	0x4	0x0	0x3	WA	0	0	4
.tbss	NOBITS	0x337c4	0x237c4	0x8	0x0	0x403	WAT	0	0	4
.init_array	INIT_ARRAY	0x337c4	0x237c4	0x4	0x0	0x3	WA	0	0	4
.fini_array	FINI_ARRAY	0x337c8	0x237c8	0x4	0x0	0x3	WA	0	0	4
.got	PROGBITS	0x337d0	0x237d0	0xa8	0x4	0x3	WA	0	0	4
.data	PROGBITS	0x33878	0x23878	0x32c	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x33ba4	0x23ba4	0x2fe8	0x0	0x3	WA	0	0	4
.ARM.attributes	ARM_ATTRIBUTES	0x0	0x23ba4	0x16	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x23bba	0x83	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
EXIDX	0x236a0	0x2b6a0	0x2b6a0	0x120	0x120	1.8876	0x4	R	0x4		.ARM.exidx
LOAD	0x0	0x8000	0x8000	0x237c0	0x237c0	3.4796	0x5	R E	0x8000		.init .text .fini .rodata .ARM.extab .ARM.exidx
LOAD	0x237c0	0x337c0	0x337c0	0x3e4	0x33cc	2.8178	0x6	RW	0x8000		.eh_frame .init_array .fini_array .got .data .bss
TLS	0x237c4	0x337c4	0x337c4	0x0	0x8	0.0000	0x4	R	0x4		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

No network behavior found

System Behavior

Analysis Process: qFl1WpWBiv PID: 5211 Parent PID: 5107

General

Start time:	15:18:58
Start date:	12/01/2022
Path:	/tmp/qFl1WpWBiv
Arguments:	/tmp/qFl1WpWBiv
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: qFl1WpWBiv PID: 5213 Parent PID: 5211

General

Start time:	15:18:58

Start date:	12/01/2022
Path:	/tmp/qFl1WpWBiv
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: qFl1WpWBiv PID: 5215 Parent PID: 5213

General

Start time:	15:18:58
Start date:	12/01/2022
Path:	/tmp/qFl1WpWBiv
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: qFl1WpWBiv PID: 5217 Parent PID: 5215

General

Start time:	15:18:58
Start date:	12/01/2022
Path:	/tmp/qFl1WpWBiv
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5217 Parent PID: 5215

General

Start time:	15:18:58
Start date:	12/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "mkdir /psl1jjs2d3/ && >/psl1jjs2d3/psl1jjs2d3 && cd /psl1jjs2d3/ >/dev/null"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5219 Parent PID: 5217

General

Start time:	15:18:58
Start date:	12/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: mkdir PID: 5219 Parent PID: 5217

General

Start time:	15:18:58
Start date:	12/01/2022
Path:	/usr/bin/mkdir
Arguments:	mkdir /psl1jjs2d3/
File size:	88408 bytes
MD5 hash:	088c9d1df5a28ed16c726eca15964cb7

File Activities

File Read

Directory Created

Analysis Process: qFl1WpWBiv PID: 5220 Parent PID: 5215

General

Start time:	15:18:58
Start date:	12/01/2022
Path:	/tmp/qFl1WpWBiv
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: sh PID: 5220 Parent PID: 5215

General

Start time:	15:18:58
Start date:	12/01/2022
Path:	/bin/sh
Arguments:	/bin/sh -c "mv /tmp/qFl1WpWBiv /psl1jjs2d3/psl1jjs2d3 && chmod 777 /psl1jjs2d3/psl1jjs2d3 >/dev/null"
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: sh PID: 5222 Parent PID: 5220

General

Start time:	15:18:58
Start date:	12/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: mv PID: 5222 Parent PID: 5220

General

Start time:	15:18:58
Start date:	12/01/2022
Path:	/usr/bin/mv
Arguments:	mv /tmp/qFl1WpWBiv /psl1jjs2d3/psl1jjs2d3
File size:	149888 bytes
MD5 hash:	504f0590fa482d4da070a702260e3716

File Activities

File Read

File Moved

Analysis Process: sh PID: 5223 Parent PID: 5220

General

Start time:	15:18:58
Start date:	12/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: chmod PID: 5223 Parent PID: 5220

General

Start time:	15:18:58
Start date:	12/01/2022
Path:	/usr/bin/chmod
Arguments:	chmod 777 /psl1jjs2d3/psl1jjs2d3
File size:	63864 bytes
MD5 hash:	739483b900c045ae1374d6f53a86a279

File Activities

File Read

Permission Modified

Analysis Process: qFl1WpWBiv PID: 5224 Parent PID: 5215

General

Start time:	15:18:59
Start date:	12/01/2022
Path:	/tmp/qFl1WpWBiv
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: qFl1WpWBiv PID: 5226 Parent PID: 5215

General

Start time:	15:18:59
Start date:	12/01/2022
Path:	/tmp/qFl1WpWBiv
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

Directory Enumerated

Analysis Process: qFl1WpWBiv PID: 5227 Parent PID: 5215

General

Start time:	15:18:59
Start date:	12/01/2022
Path:	/tmp/qFl1WpWBiv
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: qFl1WpWBiv PID: 5381 Parent PID: 5227

General

Start time:	15:20:35
Start date:	12/01/2022
Path:	/tmp/qFl1WpWBiv
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: dash PID: 5240 Parent PID: 4331

General

Start time:	15:19:18
Start date:	12/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: 5240 Parent PID: 4331

General

Start time:	15:19:18
Start date:	12/01/2022
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.cKEJqxaxsv
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: 5241 Parent PID: 4331

General

Start time:	15:19:18
Start date:	12/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 5241 Parent PID: 4331

General

Start time:	15:19:18
Start date:	12/01/2022
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: 5242 Parent PID: 4331

General

Start time:	15:19:18
Start date:	12/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 5242 Parent PID: 4331

General

Start time:	15:19:18
Start date:	12/01/2022
Path:	/usr/bin/tr
Arguments:	tr -d \\000-\\011\\013\\014\\016-\\037
File size:	51544 bytes
MD5 hash:	fbd1402dd9f72d8ebfff00ce7c3a7bb5

File Activities

File Read

Analysis Process: dash PID: 5243 Parent PID: 4331

General

Start time:	15:19:18
Start date:	12/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: 5243 Parent PID: 4331

General

Start time:	15:19:18
Start date:	12/01/2022
Path:	/usr/bin/cut
Arguments:	cut -c -80
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

Analysis Process: dash PID: 5244 Parent PID: 4331

General

Start time:	15:19:18
Start date:	12/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cat PID: 5244 Parent PID: 4331

General

Start time:	15:19:18
Start date:	12/01/2022
Path:	/usr/bin/cat
Arguments:	cat /tmp/tmp.cKEJqxaxsv
File size:	43416 bytes
MD5 hash:	7e9d213e404ad3bb82e4ebb2e1f2c1b3

File Activities

File Read

Analysis Process: dash PID: 5245 Parent PID: 4331

General

Start time:	15:19:18
Start date:	12/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: head PID: 5245 Parent PID: 4331

General

Start time:	15:19:18
Start date:	12/01/2022
Path:	/usr/bin/head
Arguments:	head -n 10
File size:	47480 bytes
MD5 hash:	fd96a67145172477dd57131396fc9608

File Activities

File Read

Analysis Process: dash PID: 5246 Parent PID: 4331

General

Start time:	15:19:18
Start date:	12/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: tr PID: 5246 Parent PID: 4331

General

Start time:	15:19:18
Start date:	12/01/2022
Path:	/usr/bin/tr

Arguments:	tr -d \\000-\\011\\013\\014\\016-\\037
File size:	51544 bytes
MD5 hash:	fbd1402dd9f72d8ebfff00ce7c3a7bb5

File Activities

File Read

Analysis Process: dash PID: 5247 Parent PID: 4331

General

Start time:	15:19:18
Start date:	12/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: cut PID: 5247 Parent PID: 4331

General

Start time:	15:19:18
Start date:	12/01/2022
Path:	/usr/bin/cut
Arguments:	cut -c -80
File size:	47480 bytes
MD5 hash:	d8ed0ea8f22c0de0f8692d4d9f1759d3

File Activities

File Read

File Written

Analysis Process: dash PID: 5248 Parent PID: 4331

General

Start time:	15:19:18
Start date:	12/01/2022
Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5248 Parent PID: 4331

General

Start time:	15:19:18
Start date:	12/01/2022
Path:	/usr/bin/rm

Arguments:	rm -f /tmp/tmp.cKEJqxaxsv /tmp/tmp.o57W8c2jCH /tmp/tmp.9D8VQf5YAB
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read

Analysis Process: systemd PID: 5283 Parent PID: 1

General

Start time:	15:19:37
Start date:	12/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: rsyslogd PID: 5283 Parent PID: 1

General

Start time:	15:19:37
Start date:	12/01/2022
Path:	/usr/sbin/rsyslogd
Arguments:	/usr/sbin/rsyslogd -n -iNONE
File size:	727248 bytes
MD5 hash:	0b8087fc907c42eb3c81a691db258e33

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: systemd PID: 5308 Parent PID: 1

General

Start time:	15:19:48
Start date:	12/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: whoopsie PID: 5308 Parent PID: 1

General

Start time:	15:19:48
Start date:	12/01/2022
Path:	/usr/bin/whoopsie
Arguments:	/usr/bin/whoopsie -f
File size:	68592 bytes
MD5 hash:	d3a6915d0e7398fb4c89a037c13959c8

File Activities

File Read

File Written

File Moved

Directory Enumerated

Directory Created

Permission Modified

Analysis Process: gdm3 PID: 5319 Parent PID: 1320

General

Start time:	15:20:07
Start date:	12/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5319 Parent PID: 1320

General

Start time:	15:20:07
Start date:	12/01/2022
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: 5338 Parent PID: 1320

General

Start time:	15:20:07
Start date:	12/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes

MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5338 Parent PID: 1320

General

Start time:	15:20:07
Start date:	12/01/2022
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: 5346 Parent PID: 1860

General

Start time:	15:20:23
Start date:	12/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5346 Parent PID: 1860

General

Start time:	15:20:23
Start date:	12/01/2022
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: 5352 Parent PID: 1

General

Start time:	15:20:27
Start date:	12/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: accounts-daemon PID: 5352 Parent PID: 1

General

Start time:	15:20:27
Start date:	12/01/2022
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: 5367 Parent PID: 5352

General

Start time:	15:20:29
Start date:	12/01/2022
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: 5367 Parent PID: 5352

General

Start time:	15:20:29
Start date:	12/01/2022
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: 5368 Parent PID: 5367

General

Start time:	15:20:30
Start date:	12/01/2022
Path:	/usr/share/language-tools/language-validate
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: language-options PID: 5368 Parent PID: 5367

General

Start time:	15:20:30
Start date:	12/01/2022
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: 5369 Parent PID: 5368

General

Start time:	15:20:30
Start date:	12/01/2022
Path:	/usr/share/language-tools/language-options
Arguments:	n/a
File size:	3478464 bytes
MD5 hash:	16a21f464119ea7fad1d3660de963637

Analysis Process: sh PID: 5369 Parent PID: 5368

General

Start time:	15:20:30
Start date:	12/01/2022
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: 5370 Parent PID: 5369

General

Start time:	15:20:30
Start date:	12/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: locale PID: 5370 Parent PID: 5369

General

Start time:	15:20:30
Start date:	12/01/2022
Path:	/usr/bin/locale
Arguments:	locale -a
File size:	58944 bytes
MD5 hash:	c72a78792469db86d91369c9057f20d2

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5371 Parent PID: 5369

General

Start time:	15:20:30
Start date:	12/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: grep PID: 5371 Parent PID: 5369

General

Start time:	15:20:30
Start date:	12/01/2022
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: 5363 Parent PID: 1809

General

Start time:	15:20:27
Start date:	12/01/2022
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	n/a
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

Analysis Process: Default PID: 5363 Parent PID: 1809

General

Start time:	15:20:27
Start date:	12/01/2022
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: 5374 Parent PID: 1320

General

Start time:	15:20:33
Start date:	12/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: gdm-session-worker PID: 5374 Parent PID: 1320

General

Start time:	15:20:33
Start date:	12/01/2022
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: 5385 Parent PID: 5374

General

Start time:	15:20:38
Start date:	12/01/2022
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	n/a
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

Analysis Process: gdm-wayland-session PID: 5385 Parent PID: 5374

General

Start time:	15:20:38
Start date:	12/01/2022
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: 5388 Parent PID: 5385

General

Start time:	15:20:39
Start date:	12/01/2022
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: 5388 Parent PID: 5385

General

Start time:	15:20:39
Start date:	12/01/2022

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: 5389 Parent PID: 5388

General

Start time:	15:20:40
Start date:	12/01/2022
Path:	/usr/bin/dbus-run-session
Arguments:	n/a
File size:	14480 bytes
MD5 hash:	245f3ef6a268850b33b0225a8753b7f4

Analysis Process: dbus-daemon PID: 5389 Parent PID: 5388

General

Start time:	15:20:40
Start date:	12/01/2022
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: 5416 Parent PID: 5389

General

Start time:	15:20:45
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5417 Parent PID: 5416

General

Start time:	15:20:45
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5417 Parent PID: 5416

General

Start time:	15:20:46
Start date:	12/01/2022
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5419 Parent PID: 5389

General

Start time:	15:20:46
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5420 Parent PID: 5419

General

Start time:	15:20:46
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5420 Parent PID: 5419

General

Start time:	15:20:46
Start date:	12/01/2022
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5421 Parent PID: 5389

General

Start time:	15:20:46
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5422 Parent PID: 5421

General

Start time:	15:20:46
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5422 Parent PID: 5421

General

Start time:	15:20:46
Start date:	12/01/2022
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5426 Parent PID: 5389

General

Start time:	15:20:46
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5427 Parent PID: 5426

General

Start time:	15:20:46
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5427 Parent PID: 5426

General

Start time:	15:20:46
Start date:	12/01/2022
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5428 Parent PID: 5389

General

Start time:	15:20:46
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5429 Parent PID: 5428

General

Start time:	15:20:46
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5429 Parent PID: 5428

General

Start time:	15:20:46
Start date:	12/01/2022
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5430 Parent PID: 5389

General

Start time:	15:20:46
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

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

General

Start time:	15:20:46
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5431 Parent PID: 5430

General

Start time:	15:20:46
Start date:	12/01/2022
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5433 Parent PID: 5389

General

Start time:	15:20:46
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5434 Parent PID: 5433

General

Start time:	15:20:46
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5434 Parent PID: 5433

General

Start time:	15:20:46
Start date:	12/01/2022
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-run-session PID: 5391 Parent PID: 5388

General

Start time:	15:20:41
Start date:	12/01/2022
Path:	/usr/bin/dbus-run-session
Arguments:	n/a
File size:	14480 bytes
MD5 hash:	245f3ef6a268850b33b0225a8753b7f4

Analysis Process: gnome-session PID: 5391 Parent PID: 5388

General

Start time:	15:20:41
Start date:	12/01/2022
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: 5391 Parent PID: 5388

General

Start time:	15:20:42
Start date:	12/01/2022
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: 5435 Parent PID: 5391

General

Start time:	15:20:47
Start date:	12/01/2022
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: 5435 Parent PID: 5391

General

Start time:	15:20:47
Start date:	12/01/2022
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: 5438 Parent PID: 5391

General

Start time:	15:20:48
Start date:	12/01/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 5438 Parent PID: 5391

General

Start time:	15:20:48
Start date:	12/01/2022
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: 5438 Parent PID: 5391

General

Start time:	15:20:48
Start date:	12/01/2022
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: 5377 Parent PID: 1320

General

Start time:	15:20:33
Start date:	12/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5377 Parent PID: 1320

General

Start time:	15:20:33
Start date:	12/01/2022
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

File Activities

File Read

Analysis Process: gvfsd-fuse PID: 5396 Parent PID: 2038

General

Start time:	15:20:43
Start date:	12/01/2022
Path:	/usr/libexec/gvfsd-fuse
Arguments:	n/a
File size:	47632 bytes

MD5 hash:	d18fbf1cbf8eb57b17fac48b7b4be933

Analysis Process: fusermount PID: 5396 Parent PID: 2038

General

Start time:	15:20:43
Start date:	12/01/2022
Path:	/bin/fusermount
Arguments:	fusermount -u -q -z -- /run/user/1000/gvfs
File size:	39144 bytes
MD5 hash:	576a1b135c82bdcbc97a91acea900566

File Activities

File Read

Analysis Process: systemd PID: 5407 Parent PID: 1

General

Start time:	15:20:45
Start date:	12/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-user-runtime-dir PID: 5407 Parent PID: 1

General

Start time:	15:20:45
Start date:	12/01/2022
Path:	/lib/systemd/systemd-user-runtime-dir
Arguments:	/lib/systemd/systemd-user-runtime-dir stop 1000
File size:	22672 bytes
MD5 hash:	d55f4b0847f88131dbcfb07435178e54

File Activities

File Deleted

File Read

Directory Enumerated

Directory Deleted

Analysis Process: gdm3 PID: 5461 Parent PID: 1320

General

Start time:	15:20:52

Start date:	12/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: gdm-session-worker PID: 5461 Parent PID: 1320

General

Start time:	15:20:52
Start date:	12/01/2022
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: 5469 Parent PID: 5461

General

Start time:	15:20:53
Start date:	12/01/2022
Path:	/usr/lib/gdm3/gdm-session-worker
Arguments:	n/a
File size:	293360 bytes
MD5 hash:	692243754bd9f38fe9bd7e230b5c060a

Analysis Process: gdm-x-session PID: 5469 Parent PID: 5461

General

Start time:	15:20:53
Start date:	12/01/2022
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: 5471 Parent PID: 5469

General

Start time:	15:20:54
Start date:	12/01/2022
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: 5471 Parent PID: 5469

General

Start time:	15:20:54
Start date:	12/01/2022
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: 5471 Parent PID: 5469

General

Start time:	15:20:54
Start date:	12/01/2022
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: 5471 Parent PID: 5469

General

Start time:	15:20:54
Start date:	12/01/2022
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: 5480 Parent PID: 5471

General

Start time:	15:21:04
Start date:	12/01/2022
Path:	/usr/lib/xorg/Xorg
Arguments:	n/a
File size:	2448840 bytes
MD5 hash:	730cf4c45a7ee8bea88abf165463b7f8

Analysis Process: sh PID: 5480 Parent PID: 5471

General

Start time:	15:21:04
Start date:	12/01/2022
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: 5481 Parent PID: 5480

General

Start time:	15:21:04
Start date:	12/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: xkbcomp PID: 5481 Parent PID: 5480

General

Start time:	15:21:04
Start date:	12/01/2022
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: 5715 Parent PID: 5471

General

Start time:	15:21:40
Start date:	12/01/2022
Path:	/usr/lib/xorg/Xorg
Arguments:	n/a
File size:	2448840 bytes
MD5 hash:	730cf4c45a7ee8bea88abf165463b7f8

Analysis Process: sh PID: 5715 Parent PID: 5471

General

Start time:	15:21:40
Start date:	12/01/2022
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: 5716 Parent PID: 5715

General

Start time:	15:21:40
Start date:	12/01/2022
Path:	/bin/sh
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: xkbcomp PID: 5716 Parent PID: 5715

General

Start time:	15:21:40
Start date:	12/01/2022
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: 5487 Parent PID: 5469

General

Start time:	15:21:11
Start date:	12/01/2022
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: 5487 Parent PID: 5469

General

Start time:	15:21:11
Start date:	12/01/2022
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: 5488 Parent PID: 5469

General

Start time:	15:21:11
Start date:	12/01/2022
Path:	/usr/lib/gdm3/gdm-x-session
Arguments:	n/a

File size:	96944 bytes
MD5 hash:	498a824333f1c1ec7767f4612d1887cc

File Activities

Directory Enumerated

Analysis Process: dbus-run-session PID: 5488 Parent PID: 5469

General

Start time:	15:21:11
Start date:	12/01/2022
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: 5489 Parent PID: 5488

General

Start time:	15:21:11
Start date:	12/01/2022
Path:	/usr/bin/dbus-run-session
Arguments:	n/a
File size:	14480 bytes
MD5 hash:	245f3ef6a268850b33b0225a8753b7f4

Analysis Process: dbus-daemon PID: 5489 Parent PID: 5488

General

Start time:	15:21:11
Start date:	12/01/2022
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: 5505 Parent PID: 5489

General

Start time:	15:21:19
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5506 Parent PID: 5505

General

Start time:	15:21:19
Start date:	12/01/2022
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: 5506 Parent PID: 5505

General

Start time:	15:21:19
Start date:	12/01/2022
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: 5511 Parent PID: 5506

General

Start time:	15:21:20
Start date:	12/01/2022
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: 5511 Parent PID: 5506

General

Start time:	15:21:20
Start date:	12/01/2022
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: 5830 Parent PID: 5511

General

Start time:	15:21:46
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5831 Parent PID: 5830

General

Start time:	15:21:46
Start date:	12/01/2022
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: 5831 Parent PID: 5830

General

Start time:	15:21:46
Start date:	12/01/2022
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: 5535 Parent PID: 5489

General

Start time:	15:21:22
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5536 Parent PID: 5535

General

Start time:	15:21:22
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5536 Parent PID: 5535

General

Start time:	15:21:22
Start date:	12/01/2022
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5538 Parent PID: 5489

General

Start time:	15:21:22

Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5539 Parent PID: 5538

General

Start time:	15:21:22
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5539 Parent PID: 5538

General

Start time:	15:21:22
Start date:	12/01/2022
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5540 Parent PID: 5489

General

Start time:	15:21:23
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5541 Parent PID: 5540

General

Start time:	15:21:23
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a

File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5541 Parent PID: 5540

General

Start time:	15:21:23
Start date:	12/01/2022
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5542 Parent PID: 5489

General

Start time:	15:21:23
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5543 Parent PID: 5542

General

Start time:	15:21:23
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5543 Parent PID: 5542

General

Start time:	15:21:23
Start date:	12/01/2022

Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5544 Parent PID: 5489

General

Start time:	15:21:23
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5545 Parent PID: 5544

General

Start time:	15:21:23
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5545 Parent PID: 5544

General

Start time:	15:21:23
Start date:	12/01/2022
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5546 Parent PID: 5489

General

Start time:	15:21:23
Start date:	12/01/2022
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:	15:21:23
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5547 Parent PID: 5546

General

Start time:	15:21:24
Start date:	12/01/2022
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5549 Parent PID: 5489

General

Start time:	15:21:24
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5550 Parent PID: 5549

General

Start time:	15:21:24
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon

Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5550 Parent PID: 5549

General

Start time:	15:21:24
Start date:	12/01/2022
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-daemon PID: 5713 Parent PID: 5489

General

Start time:	15:21:40
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5714 Parent PID: 5713

General

Start time:	15:21:40
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: ibus-portal PID: 5714 Parent PID: 5713

General

Start time:	15:21:40

Start date:	12/01/2022
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: 5833 Parent PID: 5489

General

Start time:	15:21:47
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5834 Parent PID: 5833

General

Start time:	15:21:47
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: gjs PID: 5834 Parent PID: 5833

General

Start time:	15:21:47
Start date:	12/01/2022
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: 5899 Parent PID: 5489

General

Start time:	15:22:03
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: dbus-daemon PID: 5900 Parent PID: 5899

General

Start time:	15:22:03
Start date:	12/01/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

File Activities

File Written

Analysis Process: false PID: 5900 Parent PID: 5899

General

Start time:	15:22:03
Start date:	12/01/2022
Path:	/bin/false
Arguments:	/bin/false
File size:	39256 bytes
MD5 hash:	3177546c74e4f0062909eae43d948bfc

File Activities

File Read

Analysis Process: dbus-run-session PID: 5490 Parent PID: 5488

General

Start time:	15:21:12
Start date:	12/01/2022
Path:	/usr/bin/dbus-run-session
Arguments:	n/a
File size:	14480 bytes
MD5 hash:	245f3ef6a268850b33b0225a8753b7f4

Analysis Process: gnome-session PID: 5490 Parent PID: 5488

General

Start time:	15:21:12
Start date:	12/01/2022
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: 5490 Parent PID: 5488

General

Start time:	15:21:12
Start date:	12/01/2022
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: 5493 Parent PID: 5490

General

Start time:	15:21:12
Start date:	12/01/2022
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: 5493 Parent PID: 5490

General

Start time:	15:21:12
Start date:	12/01/2022
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: 5512 Parent PID: 5493

General

Start time:	15:21:20
Start date:	12/01/2022
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: 5512 Parent PID: 5493

General

Start time:	15:21:20
Start date:	12/01/2022
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: 5522 Parent PID: 5493

General

Start time:	15:21:21
Start date:	12/01/2022
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: 5522 Parent PID: 5493

General

Start time:	15:21:21
Start date:	12/01/2022
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: 5551 Parent PID: 5490

General

Start time:	15:21:24
Start date:	12/01/2022
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: 5551 Parent PID: 5490

General

Start time:	15:21:24
Start date:	12/01/2022
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: 5552 Parent PID: 5490

General

Start time:	15:21:25
Start date:	12/01/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

File Read

Directory Enumerated

Analysis Process: sh PID: 5552 Parent PID: 5490

General

Start time:	15:21:25
Start date:	12/01/2022
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: 5552 Parent PID: 5490

General

Start time:	15:21:25
Start date:	12/01/2022
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: 5588 Parent PID: 5552

General

Start time:	15:21:38
Start date:	12/01/2022
Path:	/usr/bin/gnome-shell
Arguments:	n/a
File size:	23168 bytes
MD5 hash:	da7a257239677622fe4b3a65972c9e87

File Activities

Directory Enumerated

Analysis Process: ibus-daemon PID: 5588 Parent PID: 5552

General

Start time:	15:21:38
Start date:	12/01/2022
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: 5708 Parent PID: 5588

General

Start time:	15:21:39
Start date:	12/01/2022
Path:	/usr/bin/ibus-daemon
Arguments:	n/a
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

File Activities

Directory Enumerated

Analysis Process: ibus-memconf PID: 5708 Parent PID: 5588

General

Start time:	15:21:40
Start date:	12/01/2022
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: 5711 Parent PID: 5588

General

Start time:	15:21:40
Start date:	12/01/2022
Path:	/usr/bin/ibus-daemon
Arguments:	n/a
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

Analysis Process: ibus-daemon PID: 5712 Parent PID: 5711

General

Start time:	15:21:40
Start date:	12/01/2022
Path:	/usr/bin/ibus-daemon
Arguments:	n/a
File size:	199088 bytes
MD5 hash:	1e00fb9860b198c73f6e364e3ff16f31

File Activities

Directory Enumerated

Analysis Process: ibus-x11 PID: 5712 Parent PID: 1

General

Start time:	15:21:40
Start date:	12/01/2022
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: 5873 Parent PID: 5588

General

Start time:	15:21:57
Start date:	12/01/2022
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: 5873 Parent PID: 5588

General

Start time:	15:21:57
Start date:	12/01/2022
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: 5854 Parent PID: 5490

General

Start time:	15:21:52
Start date:	12/01/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 5854 Parent PID: 5490

General

Start time:	15:21:52
Start date:	12/01/2022
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: 5854 Parent PID: 5490

General

Start time:	15:21:52
Start date:	12/01/2022
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: 5856 Parent PID: 5490

General

Start time:	15:21:52
Start date:	12/01/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 5856 Parent PID: 5490

General

Start time:	15:21:52
Start date:	12/01/2022
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: 5856 Parent PID: 5490

General

Start time:	15:21:53
Start date:	12/01/2022
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: 5858 Parent PID: 5490

General

Start time:	15:21:52
Start date:	12/01/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 5858 Parent PID: 5490

General

Start time:	15:21:53
Start date:	12/01/2022
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: 5858 Parent PID: 5490

General

Start time:	15:21:53
Start date:	12/01/2022
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: 5859 Parent PID: 5490

General

Start time:	15:21:53
Start date:	12/01/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 5859 Parent PID: 5490

General

Start time:	15:21:53
Start date:	12/01/2022
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

File Activities

File Read

Analysis Process: gsd-keyboard PID: 5859 Parent PID: 5490

General

Start time:	15:21:53
Start date:	12/01/2022
Path:	/usr/libexec/gsd-keyboard
Arguments:	/usr/libexec/gsd-keyboard
File size:	39760 bytes
MD5 hash:	8e288fd17c80bb0a1148b964b2ac2279

File Activities

File Read

File Written

Directory Enumerated

Directory Created

Analysis Process: gnome-session-binary PID: 5860 Parent PID: 5490

General

Start time:	15:21:53
Start date:	12/01/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

File Activities

Directory Enumerated

Analysis Process: sh PID: 5860 Parent PID: 5490

General

Start time:	15:21:53
Start date:	12/01/2022
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

File Activities

File Read

Analysis Process: gsd-print-notifications PID: 5860 Parent PID: 5490

General

Start time:	15:21:54
Start date:	12/01/2022
Path:	/usr/libexec/gsd-print-notifications
Arguments:	/usr/libexec/gsd-print-notifications
File size:	51840 bytes
MD5 hash:	71539698aa691718cee775d6b9450ae2

File Activities

File Read

Analysis Process: gsd-print-notifications PID: 6032 Parent PID: 5860

General

Start time:	15:22:05
Start date:	12/01/2022
Path:	/usr/libexec/gsd-print-notifications
Arguments:	n/a
File size:	51840 bytes
MD5 hash:	71539698aa691718cee775d6b9450ae2

Analysis Process: gsd-print-notifications PID: 6033 Parent PID: 6032

General

Start time:	15:22:05
Start date:	12/01/2022
Path:	/usr/libexec/gsd-print-notifications
Arguments:	n/a
File size:	51840 bytes
MD5 hash:	71539698aa691718cee775d6b9450ae2

File Activities

Directory Enumerated

Analysis Process: gsd-printer PID: 6033 Parent PID: 1

General

Start time:	15:22:06
Start date:	12/01/2022
Path:	/usr/libexec/gsd-printer
Arguments:	/usr/libexec/gsd-printer
File size:	31120 bytes
MD5 hash:	7995828cf98c315fd55f2ffb3b22384d

Analysis Process: gnome-session-binary PID: 5861 Parent PID: 5490

General

Start time:	15:21:54
Start date:	12/01/2022
Path:	/usr/libexec/gnome-session-binary

Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 5861 Parent PID: 5490

General

Start time:	15:21:54
Start date:	12/01/2022
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: 5861 Parent PID: 5490

General

Start time:	15:21:54
Start date:	12/01/2022
Path:	/usr/libexec/gsd-rfkill
Arguments:	/usr/libexec/gsd-rfkill
File size:	51808 bytes
MD5 hash:	88a16a3c0aba1759358c06215ecfb5cc

Analysis Process: gnome-session-binary PID: 5863 Parent PID: 5490

General

Start time:	15:21:54
Start date:	12/01/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 5863 Parent PID: 5490

General

Start time:	15:21:54
Start date:	12/01/2022
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: 5863 Parent PID: 5490

General

Start time:	15:21:54

Start date:	12/01/2022
Path:	/usr/libexec/gsd-smartcard
Arguments:	/usr/libexec/gsd-smartcard
File size:	109152 bytes
MD5 hash:	ea1fbd7f62e4cd0331eae2ef754ee605

Analysis Process: gnome-session-binary PID: 5864 Parent PID: 5490

General

Start time:	15:21:54
Start date:	12/01/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 5864 Parent PID: 5490

General

Start time:	15:21:54
Start date:	12/01/2022
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: 5864 Parent PID: 5490

General

Start time:	15:21:55
Start date:	12/01/2022
Path:	/usr/libexec/gsd-datetime
Arguments:	/usr/libexec/gsd-datetime
File size:	76736 bytes
MD5 hash:	d80d39745740de37d6634d36e344d4bc

Analysis Process: gnome-session-binary PID: 5866 Parent PID: 5490

General

Start time:	15:21:55
Start date:	12/01/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 5866 Parent PID: 5490

General

Start time:	15:21:55
Start date:	12/01/2022
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: 5866 Parent PID: 5490

General

Start time:	15:21:56
Start date:	12/01/2022
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: 5867 Parent PID: 5490

General

Start time:	15:21:55
Start date:	12/01/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 5867 Parent PID: 5490

General

Start time:	15:21:56
Start date:	12/01/2022
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: 5867 Parent PID: 5490

General

Start time:	15:21:56
Start date:	12/01/2022
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: 5868 Parent PID: 5490

General

Start time:	15:21:56
Start date:	12/01/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 5868 Parent PID: 5490

General

Start time:	15:21:56
Start date:	12/01/2022
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: 5868 Parent PID: 5490

General

Start time:	15:21:57
Start date:	12/01/2022
Path:	/usr/libexec/gsd-sound
Arguments:	/usr/libexec/gsd-sound
File size:	31248 bytes
MD5 hash:	4c7d3fb993463337b4a0eb5c80c760ee

Analysis Process: gnome-session-binary PID: 5872 Parent PID: 5490

General

Start time:	15:21:56
Start date:	12/01/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 5872 Parent PID: 5490

General

Start time:	15:21:57
Start date:	12/01/2022
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: 5872 Parent PID: 5490

General

Start time:	15:21:58
Start date:	12/01/2022
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: 5875 Parent PID: 5490

General

Start time:	15:21:57
Start date:	12/01/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 5875 Parent PID: 5490

General

Start time:	15:21:58
Start date:	12/01/2022
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: 5875 Parent PID: 5490

General

Start time:	15:21:58
Start date:	12/01/2022
Path:	/usr/libexec/gsd-housekeeping
Arguments:	/usr/libexec/gsd-housekeeping
File size:	51840 bytes
MD5 hash:	b55f3394a84976ddb92a2915e5d76914

Analysis Process: gnome-session-binary PID: 5880 Parent PID: 5490

General

Start time:	15:21:58
Start date:	12/01/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 5880 Parent PID: 5490

General

Start time:	15:21:58
Start date:	12/01/2022
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: 5880 Parent PID: 5490

General

Start time:	15:21:59
Start date:	12/01/2022
Path:	/usr/libexec/gsd-power
Arguments:	/usr/libexec/gsd-power
File size:	88672 bytes
MD5 hash:	28b8e1b43c3e7f1db6741ea1ecd978b7

Analysis Process: gnome-session-binary PID: 6335 Parent PID: 5490

General

Start time:	15:22:31
Start date:	12/01/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 6335 Parent PID: 5490

General

Start time:	15:22:32
Start date:	12/01/2022
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: 6335 Parent PID: 5490

General

Start time:	15:22:32
Start date:	12/01/2022
Path:	/usr/bin/spice-vdagent
Arguments:	/usr/bin/spice-vdagent
File size:	80664 bytes
MD5 hash:	80fb7f613aa78d1b8a229dbcf4577a9d

Analysis Process: gnome-session-binary PID: 6340 Parent PID: 5490

General

Start time:	15:22:34
Start date:	12/01/2022
Path:	/usr/libexec/gnome-session-binary
Arguments:	n/a
File size:	334664 bytes
MD5 hash:	d9b90be4f7db60cb3c2d3da6a1d31bfb

Analysis Process: sh PID: 6340 Parent PID: 5490

General

Start time:	15:22:34
Start date:	12/01/2022
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: 6340 Parent PID: 5490

General

Start time:	15:22:34
Start date:	12/01/2022
Path:	/usr/bin/xbrlapi
Arguments:	xbrlapi -q
File size:	166384 bytes
MD5 hash:	0cfe25df39d38af32d6265ed947ca5b9

Analysis Process: gdm3 PID: 5462 Parent PID: 1320

General

Start time:	15:20:52
Start date:	12/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5462 Parent PID: 1320

General

Start time:	15:20:52
Start date:	12/01/2022
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes

MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: gdm3 PID: 5463 Parent PID: 1320

General

Start time:	15:20:52
Start date:	12/01/2022
Path:	/usr/sbin/gdm3
Arguments:	n/a
File size:	453296 bytes
MD5 hash:	2492e2d8d34f9377e3e530a61a15674f

Analysis Process: Default PID: 5463 Parent PID: 1320

General

Start time:	15:20:52
Start date:	12/01/2022
Path:	/etc/gdm3/PrimeOff/Default
Arguments:	/etc/gdm3/PrimeOff/Default
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: systemd PID: 5577 Parent PID: 1

General

Start time:	15:21:39
Start date:	12/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-localed PID: 5577 Parent PID: 1

General

Start time:	15:21:39
Start date:	12/01/2022
Path:	/lib/systemd/systemd-localed
Arguments:	/lib/systemd/systemd-localed
File size:	43232 bytes
MD5 hash:	1244af9646256d49594f2a8203329aa9

Analysis Process: systemd PID: 5724 Parent PID: 1334

General

Start time:	15:21:44
Start date:	12/01/2022
Path:	/usr/lib/systemd/systemd

Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: pulseaudio PID: 5724 Parent PID: 1334

General

Start time:	15:21:44
Start date:	12/01/2022
Path:	/usr/bin/pulseaudio
Arguments:	/usr/bin/pulseaudio --daemonize=no --log-target=journal
File size:	100832 bytes
MD5 hash:	0c3b4c789d8ffb12b25507f27e14c186

Analysis Process: systemd PID: 5725 Parent PID: 1

General

Start time:	15:21:45
Start date:	12/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: geoclue PID: 5725 Parent PID: 1

General

Start time:	15:21:45
Start date:	12/01/2022
Path:	/usr/libexec/geoclue
Arguments:	/usr/libexec/geoclue
File size:	301544 bytes
MD5 hash:	30ac5455f3c598dde91dc87477fb19f7

Analysis Process: systemd PID: 5901 Parent PID: 1

General

Start time:	15:22:03
Start date:	12/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-hostnamed PID: 5901 Parent PID: 1

General

Start time:	15:22:03

Start date:	12/01/2022
Path:	/lib/systemd/systemd-hostnamed
Arguments:	/lib/systemd/systemd-hostnamed
File size:	35040 bytes
MD5 hash:	2cc8a5576629a2d5bd98e49a4b8bef65

Analysis Process: systemd PID: 6076 Parent PID: 1

General

Start time:	15:22:18
Start date:	12/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: fprintd PID: 6076 Parent PID: 1

General

Start time:	15:22:18
Start date:	12/01/2022
Path:	/usr/libexec/fprintd
Arguments:	/usr/libexec/fprintd
File size:	125312 bytes
MD5 hash:	b0d8829f05cd028529b84b061b660e84

Analysis Process: systemd PID: 6201 Parent PID: 1

General

Start time:	15:22:26
Start date:	12/01/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: systemd-localed PID: 6201 Parent PID: 1

General

Start time:	15:22:26
Start date:	12/01/2022
Path:	/lib/systemd/systemd-localed
Arguments:	/lib/systemd/systemd-localed
File size:	43232 bytes
MD5 hash:	1244af9646256d49594f2a8203329aa9