FINITE STATE

Project Risk Report

Project Name:
Reachability Sample

Version:
1.0

Organization:
Fs-Yolo

Published: **2025-07-25**

INTRODUCTION

About Finite State

Finite State was founded to protect the devices that power our modern lives by illuminating the vulnerabilities and threats within their complex software supply chains. We recognize that supply chain security is the #1 problem in cyber security today. Global software supply chains are opaque and complicated, involving countless developers, vendors, and components. Malicious actors exploit supply chain vulnerabilities to gain access to the networks that power our critical infrastructure and can carry out potentially devastating attacks.

Finite State defends these critical devices, networks, and supply chains by leveraging massive data analysis of device firmware and software to provide transparency to device manufacturers and their customers - enabling them to understand and mitigate their risks before they are compromised.

This report by Finite State provides comprehensive security analysis of your product and its firmware. Combined, this provides insight into the firmware and its vulnerabilities to help protect and secure your mission critical products.

Confidentiality and Privacy

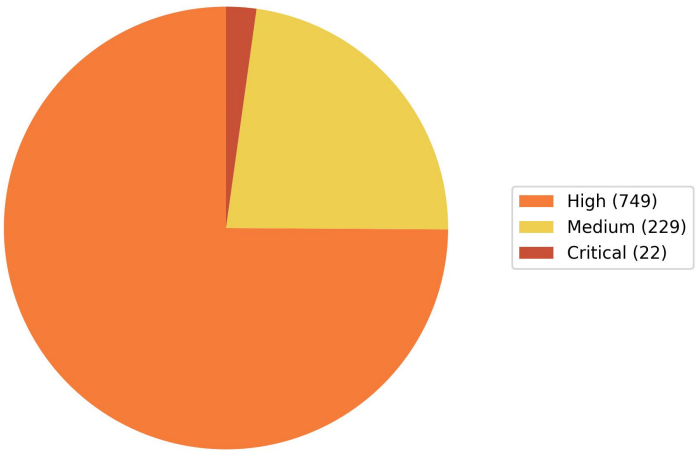
Finite State, Inc., ("Finite State," "we," or "us") respects the privacy of our customers, business partners, event attendees, job applicants, and visitors to Finite State websites ("Sites"). We recognize the need for appropriate protections and management of personal information that is shared with and provided to Finite State. Finite State has developed this Privacy Policy to assist you to understand what personal information Finite State collects and how that personal information is used. It also describes your choices regarding the use, access and correction of your personal information. This Privacy Policy applies to Sites operated by Finite State such as www.finitestate.io and other webpages in which we post and directly link to this policy.

EXECUTIVE SUMMARY

This report provides a comprehensive security assessment of **Reachability Sample** version **1.0**. The analysis identified **186 software components** and **2,677 security findings** across the project.

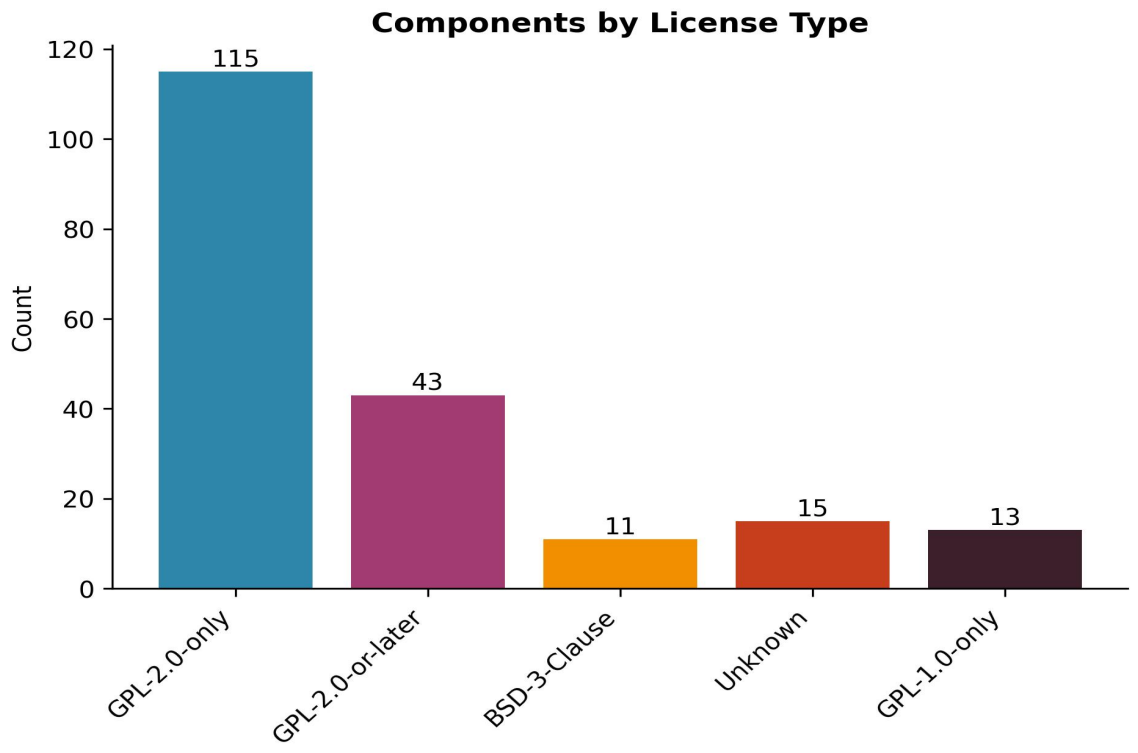
186	2677	22	749	229	0
Total Components	Total Findings	Critical	High	Medium	Low

RISK OVERVIEW



COMPONENT ANALYSIS

The analysis identified **186 software components** within the project. These components have been analyzed for licensing and security vulnerabilities.



COMPONENT RISK ANALYSIS

The following components have been identified as the highest risk based on their vulnerability counts, severity levels, and policy compliance issues. These components should be prioritized for remediation.

Component	Version	Critical	High	Medium	Low	Violations	Warnings
Linux	3.10.108	22	749	1818	81	72	1870
cls_flow		0	0	0	0	0	0
nls_cp936		0	0	0	0	0	0
krng		0	0	0	0	0	0
ip6table_nat		0	0	0	0	0	0
pcompress		0	0	0	0	0	0
ip6table_raw		0	0	0	0	0	0
crc32		0	0	0	0	0	0
authenc		0	0	0	0	0	0
crypto_blkcipher		0	0	0	0	0	0

REACHABILITY ANALYSIS

The analysis identified **89 reachable findings** and **1828 unreachable findings**. Reachable findings indicate vulnerabilities that are potentially accessible in the codebase, while unreachable findings are not accessible.

Top 100

#	Finding ID	Component	Severity	Result	Score	Risk
1	CVE-2022-27666	Linux	High	Reachable	100	7.8
2	CVE-2024-35896	Linux	High	Reachable	100	7.1
3	CVE-2025-21764	Linux	High	Reachable	50	7.8
4	CVE-2025-21760	Linux	High	Reachable	50	7.8
5	CVE-2025-21759	Linux	High	Reachable	50	7.8
6	CVE-2024-56606	Linux	High	Reachable	50	7.8
7	CVE-2024-56600	Linux	High	Reachable	50	7.8
8	CVE-2024-47742	Linux	High	Reachable	50	7.8
9	CVE-2024-46744	Linux	High	Reachable	50	7.8
10	CVE-2024-44987	Linux	High	Reachable	50	7.8
11	CVE-2024-26882	Linux	High	Reachable	50	7.8
12	CVE-2021-47634	Linux	High	Reachable	50	7.8
13	CVE-2021-47103	Linux	High	Reachable	50	7.8
14	CVE-2021-22555	Linux	High	Reachable	50	7.8
15	CVE-2017-9077	Linux	High	Reachable	50	7.8
16	CVE-2017-18509	Linux	High	Reachable	50	7.8
17	CVE-2017-17806	Linux	High	Reachable	50	7.8
18	CVE-2017-16939	Linux	High	Reachable	50	7.8
19	CVE-2017-15649	Linux	High	Reachable	50	7.8
20	CVE-2016-9755	Linux	High	Reachable	50	7.8
21	CVE-2023-52340	Linux	High	Reachable	50	7.5
22	CVE-2022-36946	Linux	High	Reachable	50	7.5
23	CVE-2025-21920	Linux	High	Reachable	50	7.1
24	CVE-2024-50035	Linux	High	Reachable	50	7.1
25	CVE-2024-50033	Linux	High	Reachable	50	7.1
26	CVE-2024-38538	Linux	High	Reachable	50	7.1
27	CVE-2024-26982	Linux	High	Reachable	50	7.1
28	CVE-2022-1353	Linux	High	Reachable	50	7.1

29	CVE-2023-52578	Linux	High	Reachable	50	7.0
30	CVE-2024-50038	Linux	Medium	Reachable	300	5.5
31	CVE-2018-1065	Linux	Medium	Reachable	100	4.7
32	CVE-2024-42229	Linux	Medium	Reachable	100	4.1
33	CVE-2013-4470	Linux	Medium	Reachable	50	6.9
34	CVE-2021-0920	Linux	Medium	Reachable	50	6.4
35	CVE-2013-4312	Linux	Medium	Reachable	50	6.2
36	CVE-2014-2309	Linux	Medium	Reachable	50	6.1
37	CVE-2013-4387	Linux	Medium	Reachable	50	6.1
38	CVE-2020-25211	Linux	Medium	Reachable	50	6.0
39	CVE-2025-21922	Linux	Medium	Reachable	50	5.5
40	CVE-2024-57996	Linux	Medium	Reachable	50	5.5
41	CVE-2024-50304	Linux	Medium	Reachable	50	5.5
42	CVE-2024-50142	Linux	Medium	Reachable	50	5.5
43	CVE-2024-49940	Linux	Medium	Reachable	50	5.5
44	CVE-2024-40960	Linux	Medium	Reachable	50	5.5
45	CVE-2024-40959	Linux	Medium	Reachable	50	5.5
46	CVE-2024-36902	Linux	Medium	Reachable	50	5.5
47	CVE-2024-36901	Linux	Medium	Reachable	50	5.5
48	CVE-2024-36286	Linux	Medium	Reachable	50	5.5
49	CVE-2024-35969	Linux	Medium	Reachable	50	5.5
50	CVE-2024-35945	Linux	Medium	Reachable	50	5.5
51	CVE-2024-26973	Linux	Medium	Reachable	50	5.5
52	CVE-2024-26675	Linux	Medium	Reachable	50	5.5
53	CVE-2024-26635	Linux	Medium	Reachable	50	5.5
54	CVE-2024-25740	Linux	Medium	Reachable	50	5.5
55	CVE-2024-25739	Linux	Medium	Reachable	50	5.5
56	CVE-2023-52449	Linux	Medium	Reachable	50	5.5
57	CVE-2023-0394	Linux	Medium	Reachable	50	5.5
58	CVE-2022-49728	Linux	Medium	Reachable	50	5.5
59	CVE-2022-49021	Linux	Medium	Reachable	50	5.5
60	CVE-2022-48911	Linux	Medium	Reachable	50	5.5
61	CVE-2022-48839	Linux	Medium	Reachable	50	5.5
62	CVE-2022-3543	Linux	Medium	Reachable	50	5.5
63	CVE-2021-47258	Linux	Medium	Reachable	50	5.5
64	CVE-2021-47182	Linux	Medium	Reachable	50	5.5

65	CVE-2021-47146	Linux	Medium	Reachable	50	5.5
66	CVE-2021-29650	Linux	Medium	Reachable	50	5.5
67	CVE-2019-20812	Linux	Medium	Reachable	50	5.5
68	CVE-2019-20422	Linux	Medium	Reachable	50	5.5
69	CVE-2017-9242	Linux	Medium	Reachable	50	5.5
70	CVE-2017-15116	Linux	Medium	Reachable	50	5.5
71	CVE-2016-8645	Linux	Medium	Reachable	50	5.5
72	CVE-2024-26804	Linux	Medium	Reachable	50	5.3
73	CVE-2013-7446	Linux	Medium	Reachable	50	5.3
74	CVE-2016-7917	Linux	Medium	Reachable	50	5.0
75	CVE-2015-8215	Linux	Medium	Reachable	50	5.0
76	CVE-2014-8160	Linux	Medium	Reachable	50	5.0
77	CVE-2015-7799	Linux	Medium	Reachable	50	4.9
78	CVE-2013-7270	Linux	Medium	Reachable	50	4.9
79	CVE-2013-7263	Linux	Medium	Reachable	50	4.9
80	CVE-2023-53020	Linux	Medium	Reachable	50	4.7
81	CVE-2022-49344	Linux	Medium	Reachable	50	4.7
82	CVE-2019-16994	Linux	Medium	Reachable	50	4.7
83	CVE-2013-6431	Linux	Medium	Reachable	50	4.7
84	CVE-2023-7192	Linux	Medium	Reachable	50	4.4
85	CVE-2022-0494	Linux	Medium	Reachable	50	4.4
86	CVE-2020-15437	Linux	Medium	Reachable	50	4.4
87	CVE-2019-15666	Linux	Medium	Reachable	50	4.4
88	CVE-2021-38209	Linux	Low	Reachable	50	3.3
89	CVE-2015-2922	Linux	Low	Reachable	50	3.3
90	CVE-2021-47548	Linux	Critical	Unreachable	-50	9.8
91	CVE-2021-47378	Linux	Critical	Unreachable	-50	9.8
92	CVE-2019-18814	Linux	Critical	Unreachable	-50	9.8
93	CVE-2019-17133	Linux	Critical	Unreachable	-50	9.8
94	CVE-2019-16746	Linux	Critical	Unreachable	-50	9.8
95	CVE-2019-15505	Linux	Critical	Unreachable	-50	9.8
96	CVE-2017-7895	Linux	Critical	Unreachable	-50	9.8
97	CVE-2017-18174	Linux	Critical	Unreachable	-50	9.8
98	CVE-2023-52832	Linux	Critical	Unreachable	-50	9.1
99	CVE-2023-52735	Linux	Critical	Unreachable	-50	9.1
100	CVE-2021-47354	Linux	Critical	Unreachable	-50	9.1

EXPLOITS SUMMARY

The analysis found **422 findings with exploit information**. These have been categorized by exploit maturity and availability.

Exploited By Ransomware	1
Exploited By Botnet	1
Exploited By Threat Actors	7
In KEV	5
Reported in the Wild	9
Commercial Exploit	8
Weaponized	19
PoC	363

TOP SECURITY RISKS

CVE ID	Severity	Risk Score	EPSS Percentile	Component
CVE-2021-47548	Critical	9.8	17.5%	Linux
CVE-2021-47378	Critical	9.8	21.8%	Linux
CVE-2021-3773	Critical	9.8	79.6%	Linux
CVE-2019-18814	Critical	9.8	65.2%	Linux
CVE-2019-17133	Critical	9.8	81.4%	Linux
CVE-2019-16746	Critical	9.8	85.1%	Linux
CVE-2019-15505	Critical	9.8	65.8%	Linux
CVE-2019-14897	Critical	9.8	71.1%	Linux
CVE-2019-14896	Critical	9.8	81.8%	Linux

CVE-2019-14895	Critical	9.8	78.5%	Linux

DETAILED FINDINGS

This section includes Critical and High severity findings, plus Medium severity findings that have exploit information. No cap is applied to ensure all important findings are displayed.

CVE-2021-47548

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ethernet: hisilicon: hns: hns_dsaf_misc: fix a possible array overflow in hns_dsaf_ge_srst_by_port() The if statement: if (port ...
Severity: Critical
Risk Score: 9.8
EPSS Percentile: 17.5%

CVE-2021-47378

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: nvme-rdma: destroy cm id before destroy qp to avoid use after free We should always destroy cm_id before destroy qp to avoid to ge...
Severity: Critical
Risk Score: 9.8
EPSS Percentile: 21.8%

CVE-2021-3773 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A flaw in netfilter could allow a network-connected attacker to infer openvpn connection endpoint information for further use in traditional network attacks.
Severity: Critical
Risk Score: 9.8
EPSS Percentile: 79.6%

CVE-2019-18814

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 5.3.9. There is a use-after-free when aa_label_parse() fails in aa_audit_rule_init() in security/apparmor/audit.c.
Severity: Critical
Risk Score: 9.8

EPSS Percentile: 65.2%

CVE-2019-17133

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel through 5.3.2, cfg80211_mgd_wext_giwessid in net/wireless/wext-sme.c does not reject a long SSID IE, leading to a Buffer Overflow.
Severity: Critical
Risk Score: 9.8
EPSS Percentile: 81.4%

CVE-2019-16746

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in net/wireless/nl80211.c in the Linux kernel through 5.2.17. It does not check the length of variable elements in a beacon head, leading to a buffer overflow.
Severity: Critical
Risk Score: 9.8
EPSS Percentile: 85.1%

CVE-2019-15505

Unreachable

Component: Linux
Version: 3.10.108
Description: drivers/media/usb/dvb-usb/technisat-usb2.c in the Linux kernel through 5.2.9 has an out-of-bounds read via crafted USB device traffic (which may be remote via usbip or usbredir).
Severity: Critical
Risk Score: 9.8
EPSS Percentile: 65.8%

CVE-2019-14897

Component: Linux
Version: 3.10.108
Description: A stack-based buffer overflow was found in the Linux kernel, version kernel-2.6.32, in Marvell WiFi chip driver. An attacker is able to cause a denial of service (system crash) or, possibly execute ar...
Severity: Critical
Risk Score: 9.8
EPSS Percentile: 71.1%

CVE-2019-14896

Component: Linux
Version: 3.10.108

Description: A heap-based buffer overflow vulnerability was found in the Linux kernel, version kernel-2.6.32, in Marvell WiFi chip driver. A remote attacker could cause a denial of service (system crash) or, possi...
Severity: Critical
Risk Score: 9.8
EPSS Percentile: 81.8%

CVE-2019-14895

Component: Linux
Version: 3.10.108
Description: A heap-based buffer overflow was discovered in the Linux kernel, all versions 3.x.x and 4.x.x before 4.18.0, in Marvell WiFi chip driver. The flaw could occur when the station attempts a connection ne...
Severity: Critical
Risk Score: 9.8
EPSS Percentile: 78.5%

CVE-2017-7895

Unreachable

Component: Linux
Version: 3.10.108
Description: The NFSv2 and NFSv3 server implementations in the Linux kernel through 4.10.13 lack certain checks for the end of a buffer, which allows remote attackers to trigger pointer-arithmetic errors or possib...
Severity: Critical
Risk Score: 9.8
EPSS Percentile: 96.5%

CVE-2017-18174

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 4.7, the amd_gpio_remove function in drivers/pinctrl/pinctrl-amd.c calls the pinctrl_unregister function, leading to a double free.
Severity: Critical
Risk Score: 9.8
EPSS Percentile: 69.1%

CVE-2016-5344

Component: Linux
Version: 3.10.108
Description: Multiple integer overflows in the MDSS driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allow attackers to cause ...
Severity: Critical
Risk Score: 9.8
EPSS Percentile: 48.5%

CVE-2016-5343

Component: Linux
Version: 3.10.108
Description: drivers/soc/qcom/qdsp6v2/voice_svc.c in the QDSP6v2 Voice Service driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products...
Severity: Critical
Risk Score: 9.8
EPSS Percentile: 73.6%

CVE-2015-0573

Component: Linux
Version: 3.10.108
Description: drivers/media/platform/msm/broadcast/tsc.c in the TSC driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows att...
Severity: Critical
Risk Score: 9.8
EPSS Percentile: 53.2%

CVE-2014-9410

Component: Linux
Version: 3.10.108
Description: The vfe31_proc_general function in drivers/media/video/msm/vfe/msm_vfe31.c in the MSM-VFE31 driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM ...
Severity: Critical
Risk Score: 9.8
EPSS Percentile: 48.1%

CVE-2023-52832

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: don't return unset power in ieee80211_get_tx_power() We can get a UBSAN warning if ieee80211_get_tx_power() return...
Severity: Critical
Risk Score: 9.1
EPSS Percentile: 56.6%

CVE-2023-52735

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: bpf, sockmap: Don't let sock_map_{close,destroy,unhash} call itself sock_map proto callbacks should never call themselves by desig...
Severity: Critical
Risk Score: 9.1
EPSS Percentile: 7.6%

CVE-2021-47354

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/sched: Avoid data corruptions Wait for all dependencies of a job to complete before killing it to avoid data corruptions.
Severity: Critical
Risk Score: 9.1
EPSS Percentile: 19.6%

CVE-2021-47348

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Avoid HDCP over-read and corruption Instead of reading the desired 5 bytes of the actual target field, the code w...
Severity: Critical
Risk Score: 9.1
EPSS Percentile: 8.3%

CVE-2019-15926

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.2.3. Out of bounds access exists in the functions ath6kl_wmi_pstream_timeout_event_rx and ath6kl_wmi_cac_event_rx in the file drivers/net/wireless/...
Severity: Critical
Risk Score: 9.1
EPSS Percentile: 85.8%

CVE-2015-4001

Component: Linux
Version: 3.10.108
Description: Integer signedness error in the oz_hcd_get_desc_cnf function in drivers/staging/ozwpan/ozhcd.c in the OZWPAN driver in the Linux kernel through 4.0.5 allows remote attackers to cause a denial of servi...
Severity: Critical
Risk Score: 9.0
EPSS Percentile: 90.2%

CVE-2024-47659

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: smack: tcp: ipv4, fix incorrect labeling Currently, Smack mirrors the label of incoming tcp/ipv4 connections: when a label 'foo' c...
Severity: High
Risk Score: 8.8

EPSS Percentile: 69.8%

CVE-2024-25744

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 6.6.7, an untrusted VMM can trigger int80 syscall handling at any given point. This is related to arch/x86/coco/tdx/tdx.c and arch/x86/mm/mem_encrypt_amd.c.
Severity: High
Risk Score: 8.8
EPSS Percentile: 12.9%

CVE-2022-42896

Unreachable

Component: Linux
Version: 3.10.108
Description: There are use-after-free vulnerabilities in the Linux kernel's net/bluetooth/l2cap_core.c's l2cap_connect and l2cap_le_connect_req functions which may allow code execution and leaking kernel memory (r...
Severity: High
Risk Score: 8.8
EPSS Percentile: 53.3%

CVE-2021-47347

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: wl1251: Fix possible buffer overflow in wl1251_cmd_scan Function wl1251_cmd_scan calls memcpy without checking the length. Harden ...
Severity: High
Risk Score: 8.8
EPSS Percentile: 31.9%

CVE-2021-47324

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: watchdog: Fix possible use-after-free in wdt_startup() This module's remove path calls del_timer(). However, that function does no...
Severity: High
Risk Score: 8.8
EPSS Percentile: 27.8%

CVE-2021-47323

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: watchdog: sc520_wdt: Fix possible use-after-free in wdt_turnoff() This module's remove path calls del_timer(). However, that funct...
Severity: High
Risk Score: 8.8
EPSS Percentile: 27.8%

CVE-2021-3653 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A flaw was found in the KVM's AMD code for supporting SVM nested virtualization. The flaw occurs when processing the VMCB (virtual machine control block) provided by the L1 guest to spawn/handle a nes...
Severity: High
Risk Score: 8.8
EPSS Percentile: 38.0%

CVE-2019-3846 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A flaw that allowed an attacker to corrupt memory and possibly escalate privileges was found in the mwifiex kernel module while connecting to a malicious wireless network.
Severity: High
Risk Score: 8.8
EPSS Percentile: 80.1%

CVE-2019-17666

Unreachable

Component: Linux
Version: 3.10.108
Description: rtl_p2p_noa_ie in drivers/net/wireless/realtek/rtlwifi/ps.c in the Linux kernel through 5.3.6 lacks a certain upper-bound check, leading to a buffer overflow.
Severity: High
Risk Score: 8.8
EPSS Percentile: 50.4%

CVE-2019-14821

Component: Linux
Version: 3.10.108
Description: An out-of-bounds access issue was found in the Linux kernel, all versions through 5.3, in the way Linux kernel's KVM hypervisor implements the Coalesced MMIO write operation. It operates on an MMIO ri...
Severity: High
Risk Score: 8.8
EPSS Percentile: 20.0%

CVE-2019-10220

Component: Linux
Version: 3.10.108
Description: Linux kernel CIFS implementation, version 4.9.0 is vulnerable to a relative paths injection in directory entry lists.
Severity: High
Risk Score: 8.8
EPSS Percentile: 71.3%

CVE-2015-4004 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The OZWPAN driver in the Linux kernel through 4.0.5 relies on an untrusted length field during packet parsing, which allows remote attackers to obtain sensitive information from kernel memory or cause...
Severity: High
Risk Score: 8.5
EPSS Percentile: 90.5%

CVE-2024-35869

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: smb: client: guarantee refcounted children from parent session Avoid potential use-after-free bugs when walking DFS referrals, mou...
Severity: High
Risk Score: 8.4
EPSS Percentile: 1.9%

CVE-2024-26945

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: crypto: iaa - Fix nr_cpus < nr_iaa case If nr_cpus < nr_iaa, the calculated cpus_per_iaa will be 0, which causes a divide-by-0 in ...
Severity: High
Risk Score: 8.4
EPSS Percentile: 1.4%

CVE-2023-52810

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: fs/jfs: Add check for negative db_l2nbperpage l2nbperpage is log2(number of blks per page), and the minimum legal value should be ...
Severity: High
Risk Score: 8.4

EPSS Percentile: 1.3%

CVE-2023-52629

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: sh: push-switch: Reorder cleanup operations to avoid use-after-free bug The original code puts flush_work() before timer_shutdown_...
Severity: High
Risk Score: 8.4
EPSS Percentile: 2.2%

CVE-2021-47456

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: can: peak_pci: peak_pci_remove(): fix UAF When remove the module peek_pci, referencing 'chan' again after releasing 'dev' will cau...
Severity: High
Risk Score: 8.4
EPSS Percentile: 4.3%

CVE-2017-2583

Component: Linux
Version: 3.10.108
Description: The load_segment_descriptor implementation in arch/x86/kvm/emulate.c in the Linux kernel before 4.9.5 improperly emulates a "MOV SS, NULL selector" instruction, which allows guest OS users to cause a ...
Severity: High
Risk Score: 8.4
EPSS Percentile: 27.6%

CVE-2016-3134 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The netfilter subsystem in the Linux kernel through 4.5.2 does not validate certain offset fields, which allows local users to gain privileges or cause a denial of service (heap memory corruption) via...
Severity: High
Risk Score: 8.4
EPSS Percentile: 54.0%

CVE-2022-1012

Unreachable

Component: Linux
Version: 3.10.108
Description: A memory leak problem was found in the TCP source port generation algorithm in net/ipv4/tcp.c due to the small table perturb size. This flaw may allow an attacker to information leak and may cause a d...
Severity: High
Risk Score: 8.2
EPSS Percentile: 60.3%

CVE-2024-58087

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix racy issue from session lookup and expire Increment the session reference count within the lock for lookup to avoid rac...
Severity: High
Risk Score: 8.1
EPSS Percentile: 34.6%

CVE-2024-36913

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: Drivers: hv: vmbus: Leak pages if set_memory_encrypted() fails In CoCo VMs it is possible for the untrusted host to cause set_memo...
Severity: High
Risk Score: 8.1
EPSS Percentile: 16.6%

CVE-2024-36912

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: Drivers: hv: vmbus: Track decrypted status in vmbus_gpadl In CoCo VMs it is possible for the untrusted host to cause set_memory_en...
Severity: High
Risk Score: 8.1
EPSS Percentile: 14.7%

CVE-2020-28374

Unreachable

Component: Linux
Version: 3.10.108
Description: In drivers/target/target_core_xcopy.c in the Linux kernel before 5.10.7, insufficient identifier checking in the LIO SCSI target code can be used by remote attackers to read or write files via directo...
Severity: High

Risk Score: 8.1
EPSS Percentile: 55.9%

CVE-2020-14305 🔥 PoC

Component: Linux
Version: 3.10.108
Description: An out-of-bounds memory write flaw was found in how the Linux kernel's Voice Over IP H.323 connection tracking functionality handled connections on ipv6 port 1720. This flaw allows an unauthenticated ...
Severity: High
Risk Score: 8.1
EPSS Percentile: 88.2%

CVE-2019-6974 🔥 PoC

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 4.20.8, kvm_ioctl_create_device in virt/kvm/kvm_main.c mishandles reference counting because of a race condition, leading to a use-after-free.
Severity: High
Risk Score: 8.1
EPSS Percentile: 94.6%

CVE-2018-20836

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 4.20. There is a race condition in smp_task_timedout() and smp_task_done() in drivers/scsi/libsas/sas_expander.c, leading to a use-after-free.
Severity: High
Risk Score: 8.1
EPSS Percentile: 87.7%

CVE-2018-16884

Component: Linux
Version: 3.10.108
Description: A flaw was found in the Linux kernel's NFS41+ subsystem. NFS41+ shares mounted in different network namespaces at the same time can make bc_svc_process() use wrong back-channel IDs and cause a use-aft...
Severity: High
Risk Score: 8.0
EPSS Percentile: 24.2%

CVE-2017-1000251 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The native Bluetooth stack in the Linux Kernel (BlueZ), starting at the Linux kernel version 2.6.32 and up to and including 4.13.1, are vulnerable to a stack overflow vulnerability in the processing o...

Severity: High
Risk Score: 8.0
EPSS Percentile: 96.0%

CVE-2025-37838

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: HSI: ssi_protocol: Fix use after free vulnerability in ssi_protocol Driver Due to Race Condition In the ssi_protocol_probe() funct...
Severity: High
Risk Score: 7.8
EPSS Percentile: 3.7%

CVE-2025-22041

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free in ksmbd_sessions_deregister() In multichannel mode, UAF issue can occur in session_deregister when the ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 2.7%

CVE-2025-22040

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix session use-after-free in multichannel connection There is a race condition between session setup and ksmbd_sessions_de...
Severity: High
Risk Score: 7.8
EPSS Percentile: 2.7%

CVE-2025-22004

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net: atm: fix use after free in lec_send() The ->send() operation frees skb so save the length before calling ->send() to avoid a ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 2.8%

CVE-2025-21999

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: proc: fix UAF in proc_get_inode() Fix race between rmmod and /proc/XXX's inode instantiation. The bug is that pde->proc_ops don't...
Severity: High
Risk Score: 7.8
EPSS Percentile: 2.8%

CVE-2025-21969

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Fix slab-use-after-free Read in l2cap_send_cmd After the hci sync command releases l2cap_conn, the hci receive d...
Severity: High
Risk Score: 7.8
EPSS Percentile: 2.8%

CVE-2025-21811

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: nilfs2: protect access to buffers with no active references nilfs_lookup_dirty_data_buffers(), which iterates through the buffers ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.8%

CVE-2025-21796

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: nfsd: clear acl_access/acl_default after releasing them If getting acl_default fails, acl_access and acl_default will be released ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.4%

CVE-2025-21786

Unreachable

Component: Linux
Version: 3.10.108

Description: In the Linux kernel, the following vulnerability has been resolved: workqueue: Put the pwq after detaching the rescuer from the pool The commit 68f83057b913("workqueue: Reap workers via kthread_stop...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.2%

CVE-2025-21780

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: avoid buffer overflow attach in smu_sys_set_pp_table() It malicious user provides a small pptable through sysfs and th...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.3%

CVE-2025-21764

Reachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ndisc: use RCU protection in ndisc_alloc_skb() ndisc_alloc_skb() can be called without RTNL or RCU being held. Add RCU protection...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.8%

CVE-2025-21763

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: neighbour: use RCU protection in __neigh_notify() __neigh_notify() can be called without RTNL or RCU protection. Use RCU protecti...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.8%

CVE-2025-21760

Reachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ndisc: extend RCU protection in ndisc_send_skb() ndisc_send_skb() can be called without RTNL or RCU held. Acquire rcu_read_lock()...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.8%

CVE-2025-21759

Reachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ipv6: mcast: extend RCU protection in igmp6_send() igmp6_send() can be called without RTNL or RCU being held. Extend RCU protecti...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.5%

CVE-2025-21753

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: btrfs: fix use-after-free when attempting to join an aborted transaction When we are trying to join the current transaction and if...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.8%

CVE-2025-21751

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net/mlx5: HWS, change error flow on matcher disconnect Currently, when firmware failure occurs during matcher disconnect flow, the...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.7%

CVE-2025-21722

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: nilfs2: do not force clear folio if buffer is referenced Patch series "nilfs2: protect busy buffer heads from being force-cleared"...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.4%

CVE-2025-21700

Unreachable

Component: Linux
Version: 3.10.108

Description: In the Linux kernel, the following vulnerability has been resolved: net: sched: Disallow replacing of child qdisc from one parent to another Lion Ackermann was able to create a UAF which can be abus...
Severity: High
Risk Score: 7.8
EPSS Percentile: 3.6%

CVE-2024-58013

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: Bluetooth: MGMT: Fix slab-use-after-free Read in mgmt_remove_adv_monitor_sync This fixes the following crash: ==========...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.3%

CVE-2024-57980

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: media: uvcvideo: Fix double free in error path If the uvc_status_init() function fails to allocate the int_urb, it will free the d...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.8%

CVE-2024-57979

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: pps: Fix a use-after-free On a board running ntpd and gpsd, I'm seeing a consistent use-after-free in sys_exit() from gpsd when re...
Severity: High
Risk Score: 7.8
EPSS Percentile: 14.6%

CVE-2024-57896

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: btrfs: flush delalloc workers queue before stopping cleaner kthread during unmount During the unmount path, at close_ctree(), we f...
Severity: High

Risk Score: 7.8
EPSS Percentile: 7.7%

CVE-2024-57850

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: jffs2: Prevent rtime decompress memory corruption The rtime decompression routine does not fully check bounds during the entirety ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 10.6%

CVE-2024-57798

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/dp_mst: Ensure mst_primary pointer is valid in drm_dp_mst_handle_up_req() While receiving an MST up request message from one t...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.4%

CVE-2024-56784

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Adding array index check to prevent memory corruption [Why & How] Array indices out of bound caused memory corrup...
Severity: High
Risk Score: 7.8
EPSS Percentile: 11.4%

CVE-2024-56775

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix handling of plane refcount [Why] The mechanism to backup and restore plane states doesn't maintain refcount, ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.2%

CVE-2024-56759

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: btrfs: fix use-after-free when COWing tree bock and tracing is enabled When a COWing a tree block, at btrfs_cow_block(), and we ha...
Severity: High
Risk Score: 7.8
EPSS Percentile: 13.2%

CVE-2024-56619

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix potential out-of-bounds memory access in nilfs_find_entry() Syzbot reported that when searching for records in a direc...
Severity: High
Risk Score: 7.8
EPSS Percentile: 15.0%

CVE-2024-56608

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix out-of-bounds access in 'dcn21_link_encoder_create' An issue was identified in the dcn21_link_encoder_create ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 12.9%

CVE-2024-56606

Reachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: af_packet: avoid erroring out after sock_init_data() in packet_create() After sock_init_data() the allocated sk object is attached...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.7%

CVE-2024-56605

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: do not leave dangling sk pointer on error in l2cap_sock_create() bt_sock_alloc() allocates the sk object and att...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.7%

CVE-2024-56604

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: Bluetooth: RFCOMM: avoid leaving dangling sk pointer in rfcomm_sock_alloc() bt_sock_alloc() attaches allocated sk object to the pr...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.2%

CVE-2024-56603

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net: af_can: do not leave a dangling sk pointer in can_create() On error can_create() frees the allocated sk object, but sock_init...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.7%

CVE-2024-56602

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net: ieee802154: do not leave a dangling sk pointer in ieee802154_create() sock_init_data() attaches the allocated sk object to th...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.7%

CVE-2024-56601

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net: inet: do not leave a dangling sk pointer in inet_create() sock_init_data() attaches the allocated sk object to the provided s...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.7%

CVE-2024-56600

Reachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net: inet6: do not leave a dangling sk pointer in inet6_create() sock_init_data() attaches the allocated sk pointer to the provide...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.7%

CVE-2024-56598

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: jfs: array-index-out-of-bounds fix in dtReadFirst The value of stbl can be sometimes out of bounds due to a bad filesystem. Added ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.7%

CVE-2024-56596

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: jfs: fix array-index-out-of-bounds in jfs_readdir The stbl might contain some invalid values. Added a check to return error code i...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.7%

CVE-2024-56595

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: jfs: add a check to prevent array-index-out-of-bounds in dbAdjTree When the value of lp is 0 at the beginning of the for loop, it ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.7%

CVE-2024-56551

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix usage slab after free [+0.000021] BUG: KASAN: slab-use-after-free in drm_sched_entity_flush+0x6cb/0x7a0 [gpu_sch...
Severity: High

Risk Score: 7.8
EPSS Percentile: 7.5%

CVE-2024-56548

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: hfsplus: don't query the device logical block size multiple times Devices block sizes may change. One of these cases is a loop dev...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.0%

CVE-2024-54458

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: bsg: Set bsg_queue to NULL after removal Currently, this does not cause any issues, but I believe it is necessary to se...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.4%

CVE-2024-53239

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ALSA: 6fire: Release resources at card release The current 6fire code tries to release the resources right after the call of usb6f...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.1%

CVE-2024-53227

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: scsi: bfa: Fix use-after-free in bfad_im_module_exit() BUG: KASAN: slab-use-after-free in __lock_acquire+0x2aca/0x3a20 Read of siz...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.1%

CVE-2024-53197 🔥 In VulnCheck KEV

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: Fix potential out-of-bound accesses for Extigy and Mbox devices A bogus device can provide a bNumConfigurations v...
Severity: High
Risk Score: 7.8
EPSS Percentile: 48.0%

CVE-2024-53194

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: PCI: Fix use-after-free of slot->bus on hot remove Dennis reports a boot crash on recent Lenovo laptops with a USB4 dock. Since c...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.1%

CVE-2024-53179

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: smb: client: fix use-after-free of signing key Customers have reported use-after-free in @ses->auth_key.response with SMB2.1 + sig...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.9%

CVE-2024-53177

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: smb: prevent use-after-free due to open_cached_dir error paths If open_cached_dir() encounters an error parsing the lease from the...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.4%

CVE-2024-53174

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: SUNRPC: make sure cache entry

active before cache_show The function `c_show` was called with protection from RCU. This only ensure...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.1%

CVE-2024-53173

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: NFSv4.0: Fix a use-after-free problem in the asynchronous open() Yang Erkun reports that when two threads are opening files at the...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.1%

CVE-2024-53165

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: sh: intc: Fix use-after-free bug in register_intc_controller() In the error handling for this function, d is freed without ever re...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.1%

CVE-2024-53156

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: wifi: ath9k: add range check for conn_rsp_epid in htc_connect_service() I found the following bug in my fuzzer: UBSAN: array-in...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.9%

CVE-2024-53142

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: initramfs: avoid filename buffer overrun The initramfs filename field is defined in Documentation/driver-api/early-userspace/buffe...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.9%

CVE-2024-53141 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: add missing range check in bitmap_ip_uadt When tb[IPSET_ATTR_IP_TO] is not present but tb[IPSET_ATTR_CIDR] exist...
Severity: High
Risk Score: 7.8
EPSS Percentile: 3.2%

CVE-2024-53133

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Handle dml allocation failure to avoid crash [Why] In the case where a dml allocation fails for any reason, the c...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.1%

CVE-2024-53126

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: vdpa: solidrun: Fix UB bug with devres In psnet_open_pf_bar() and snet_open_vf_bar() a string later passed to pcim_iomap_regions()...
Severity: High
Risk Score: 7.8
EPSS Percentile: 3.5%

CVE-2024-53104 🔥 In VulnCheck KEV

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: media: uvcvideo: Skip parsing frames of type UVC_VS_UNDEFINED in uvc_parse_format This can lead to out of bounds writes since fram...
Severity: High
Risk Score: 7.8
EPSS Percentile: 83.5%

CVE-2024-53103

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: hv_sock: Initializing vsk->trans to NULL to prevent a dangling pointer When hvs is released, there is a possibility that vsk->tran...

Severity: High
Risk Score: 7.8
EPSS Percentile: 8.9%

CVE-2024-53098

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/xe/ufence: Prefetch ufence addr to catch bogus address access_ok() only checks for addr overflow so also try to read the addr ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.1%

CVE-2024-53057

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net/sched: stop qdisc_tree_reduce_backlog on TC_H_ROOT In qdisc_tree_reduce_backlog, Qdiscs with major handle ffff: are assumed to...
Severity: High
Risk Score: 7.8
EPSS Percentile: 13.9%

CVE-2024-50283

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix slab-use-after-free in smb3_preauth_hash_rsp ksmbd_user_session_put should be called under smb3_preauth_hash_rsp(). It ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.4%

CVE-2024-50282

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: add missing size check in amdgpu_debugfs_gprwave_read() Avoid a possible buffer overflow if size is larger than 4K. (...
Severity: High
Risk Score: 7.8
EPSS Percentile: 4.2%

CVE-2024-50267

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: USB: serial: io_edgeport: fix use after free in debug printk The "dev_dbg(&urb->dev->dev, ..." which happens after usb_free_urb(ur...
Severity: High
Risk Score: 7.8
EPSS Percentile: 13.9%

CVE-2024-50246

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: Add rough attr alloc_size check
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.1%

CVE-2024-50242

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: Additional check in ntfs_file_release
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.6%

CVE-2024-50230

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix kernel bug due to missing clearing of checked flag Syzbot reported that in directory operations after nilfs2 detects f...
Severity: High
Risk Score: 7.8
EPSS Percentile: 14.3%

CVE-2024-50180

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: fbdev: sisfb: Fix strbuf array overflow The values of the variables xres and yres are placed in strbuf. These variables are obtain...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.8%

CVE-2024-50143

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: udf: fix uninit-value use in udf_get_fileshortad Check for overflow when computing alen in udf_current_aext to mitigate later unin...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.8%

CVE-2024-50112

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: x86/lam: Disable ADDRESS_MASKING in most cases Linear Address Masking (LAM) has a weakness related to transient execution as descr...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.8%

CVE-2024-50073

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: tty: n_gsm: Fix use-after-free in gsm_cleanup_mux BUG: KASAN: slab-use-after-free in gsm_cleanup_mux+0x77b/0x7b0 drivers/tty/n_gsm...
Severity: High
Risk Score: 7.8
EPSS Percentile: 2.2%

CVE-2024-50055

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: driver core: bus: Fix double free in driver API bus_register() For bus_register(), any error which happens after kset_register() w...
Severity: High
Risk Score: 7.8

EPSS Percentile: 8.8%

CVE-2024-50051

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: spi: mpc52xx: Add cancel_work_sync before module remove If we remove the module which will call mpc52xx_spi_remove it will free 'm...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.7%

CVE-2024-50047

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: smb: client: fix UAF in async decryption Doing an async decryption (large read) crashes with a slab-use-after-free way down in the...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.6%

CVE-2024-50007

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ALSA: asihpi: Fix potential OOB array access ASIHPI driver stores some values in the static array upon a response from the driver,...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.0%

CVE-2024-49992

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/stm: Avoid use-after-free issues with crtc and plane ltdc_load() calls functions drm_crtc_init_with_planes(), drm_universal_pl...
Severity: High
Risk Score: 7.8
EPSS Percentile: 20.8%

CVE-2024-49991

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: amdkfd_free_gtt_mem clear the correct pointer Pass pointer reference to amdgpu_bo_unref to clear the correct pointer, ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.5%

CVE-2024-49989

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: fix double free issue during amdgpu module unload Flexible endpoints use DIGs from available inflexible endpoints...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.6%

CVE-2024-49969

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix index out of bounds in DCN30 color transformation This commit addresses a potential index out of bounds issue...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.5%

CVE-2024-49966

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ocfs2: cancel dqi_sync_work before freeing oinfo ocfs2_global_read_info() will initialize and schedule dqi_sync_work at the end, i...
Severity: High
Risk Score: 7.8
EPSS Percentile: 12.5%

CVE-2024-49960

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ext4: fix timer use-after-free on failed mount Syzbot has found an ODEBUG bug in ext4_fill_super The del_timer_sync function canc...
Severity: High
Risk Score: 7.8

EPSS Percentile: 8.6%

CVE-2024-49950

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Fix uaf in l2cap_connect [Syzbot reported] BUG: KASAN: slab-use-after-free in l2cap_connect.constprop.0+0x10d8/0...
Severity: High
Risk Score: 7.8
EPSS Percentile: 13.2%

CVE-2024-49936

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net/xen-netback: prevent UAF in xenvif_flush_hash() During the list_for_each_entry_rcu iteration call of xenvif_flush_hash, kfree_...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.8%

CVE-2024-49931

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: fix array out-of-bound access in SoC stats Currently, the ath12k_soc_dp_stats::hal_reo_error array is defined with a...
Severity: High
Risk Score: 7.8
EPSS Percentile: 10.0%

CVE-2024-49930

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: wifi: ath11k: fix array out-of-bound access in SoC stats Currently, the ath11k_soc_dp_stats::hal_reo_error array is defined with a...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.8%

CVE-2024-49924

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: fbdev: pxafb: Fix possible use after free in pxafb_task() In the pxafb_probe function, it calls the pxafb_init_fbinfo function, af...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.0%

CVE-2024-49895

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix index out of bounds in DCN30 degamma hardware format translation This commit addresses a potential index out ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.5%

CVE-2024-49894

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix index out of bounds in degamma hardware format translation Fixes index out of bounds issue in `cm_helper_tran...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.1%

CVE-2024-49889

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ext4: avoid use-after-free in ext4_ext_show_leaf() In ext4_find_extent(), path may be freed by error or be reallocated, so using a...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.8%

CVE-2024-49882

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ext4: fix double brelse() the buffer of the extents path In ext4_ext_try_to_merge_up(), set path[1].p_bh to NULL after it has been...
Severity: High
Risk Score: 7.8
EPSS Percentile: 12.5%

CVE-2024-47745

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: mm: call the security_mmap_file() LSM hook in remap_file_pages() The remap_file_pages syscall handler calls do_mmap() directly, wh...
Severity: High
Risk Score: 7.8
EPSS Percentile: 0.8%

CVE-2024-47742

Reachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: firmware_loader: Block path traversal Most firmware names are hardcoded strings, or are constructed from fairly constrained format...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.6%

CVE-2024-47701

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ext4: avoid OOB when system.data xattr changes underneath the filesystem When looking up for an entry in an inlined directory, if ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 12.5%

CVE-2024-47670

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ocfs2: add bounds checking to ocfs2_xattr_find_entry() Add a paranoia check to make sure it doesn't stray beyond valid memory regi...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.8%

CVE-2024-46871

Component: Linux
Version: 3.10.108

Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Correct the defined value for AMDGPU_DMUB_NOTIFICATION_MAX [Why & How] It actually exposes '6' types in enum dmub...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.8%

CVE-2024-46859

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: platform/x86: panasonic-laptop: Fix SINF array out of bounds accesses The panasonic laptop code in various places uses the SINF ar...
Severity: High
Risk Score: 7.8
EPSS Percentile: 13.7%

CVE-2024-46844

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: um: line: always fill *error_out in setup_one_line() The pointer isn't initialized by callers, but I have encountered cases where ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.8%

CVE-2024-46836

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: usb: gadget: aspeed_udc: validate endpoint index for ast udc We should verify the bound of the array to assure that host may not m...
Severity: High
Risk Score: 7.8
EPSS Percentile: 10.0%

CVE-2024-46833

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net: hns3: void array out of bound when loop tnl_num When query reg inf of SSU, it loops tnl_num times. However, tnl_num comes fro...
Severity: High

Risk Score: 7.8
EPSS Percentile: 10.0%

CVE-2024-46821

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd/pm: Fix negative array index read Avoid using the negative values for clk_idex as an index into an array pptable->DpmDescr...
Severity: High
Risk Score: 7.8
EPSS Percentile: 11.5%

CVE-2024-46818

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check gpio_id before used as array index [WHY & HOW] GPIO_ID_UNKNOWN (-1) is not a valid value for array index an...
Severity: High
Risk Score: 7.8
EPSS Percentile: 11.5%

CVE-2024-46815

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check num_valid_sets before accessing reader_wm_sets[] [WHY & HOW] num_valid_sets needs to be checked to avoid a ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.7%

CVE-2024-46814

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check msg_id before processing transcation [WHY & HOW] HDCP_MESSAGE_ID_INVALID (-1) is not a valid msg_id nor is ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 11.5%

CVE-2024-46813

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check link_index before accessing dc->links[] [WHY & HOW] dc->links[] has max size of MAX_LINKS and NULL is retur...
Severity: High
Risk Score: 7.8

EPSS Percentile: 14.9%

CVE-2024-46811

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix index may exceed array range within fpu_update_bw_bounding_box [Why] Coverity reports OVERRUN warning. soc.nu...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.1%

CVE-2024-46804

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add array index check for hdcp ddc access [Why] Coverity reports OVERRUN warning. Do not check if array index val...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.8%

CVE-2024-46800

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: sch/netem: fix use after free in netem_dequeue If netem_dequeue() enqueues packet to inner qdisc and that qdisc returns __NET_XMIT...
Severity: High
Risk Score: 7.8
EPSS Percentile: 17.2%

CVE-2024-46759

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: hwmon: (adc128d818) Fix underflows seen when writing limit attributes DIV_ROUND_CLOSEST() after kstrtol() results in an underflow ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 13.9%

CVE-2024-46746

Unreachable

Component: Linux
Version: 3.10.108

Description: In the Linux kernel, the following vulnerability has been resolved: HID: amd_sfh: free driver_data after destroying hid device HID driver callbacks aren't called anymore once hid_destroy_device() ha...
Severity: High
Risk Score: 7.8
EPSS Percentile: 20.0%

CVE-2024-46744

Reachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: Squashfs: sanity check symbolic link size Syzkiller reports a "KMSAN: uninit-value in pick_link" bug. This is caused by an uninit...
Severity: High
Risk Score: 7.8
EPSS Percentile: 10.5%

CVE-2024-46738

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: VMCI: Fix use-after-free when removing resource in vmci_resource_remove() When removing a resource from vmci_resource_table in vmc...
Severity: High
Risk Score: 7.8
EPSS Percentile: 18.4%

CVE-2024-46725

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix out-of-bounds write warning Check the ring type value to fix the out-of-bounds write warning
Severity: High
Risk Score: 7.8
EPSS Percentile: 9.9%

CVE-2024-46673

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: scsi: aacraid: Fix double-free on probe failure aac_probe_one() calls hardware-specific init functions through the aac_driver_iden...
Severity: High
Risk Score: 7.8

EPSS Percentile: 13.9%

CVE-2024-44998

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: atm: idt77252: prevent use after free in dequeue_rx() We can't dereference "skb" after calling vcc->push() because the skb is rele...
Severity: High
Risk Score: 7.8
EPSS Percentile: 10.3%

CVE-2024-44987

Reachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ipv6: prevent UAF in ip6_send_skb() syzbot reported an UAF in ip6_send_skb() [1] After ip6_local_out() has returned, we no longer...
Severity: High
Risk Score: 7.8
EPSS Percentile: 14.9%

CVE-2024-44977

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Validate TA binary size Add TA binary size validation to avoid OOB write. (cherry picked from commit c0a04e3570d72aaf...
Severity: High
Risk Score: 7.8
EPSS Percentile: 11.5%

CVE-2024-44949

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: parisc: fix a possible DMA corruption ARCH_DMA_MINALIGN was defined as 16 - this is too small - it may be possible that two unrela...
Severity: High
Risk Score: 7.8
EPSS Percentile: 9.9%

CVE-2024-44942

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to do sanity check on F2FS_INLINE_DATA flag in inode during GC syzbot reports a f2fs bug as below: ------------[cut he...
Severity: High
Risk Score: 7.8
EPSS Percentile: 10.1%

CVE-2024-44941

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to cover read extent cache access with lock syzbot reports a f2fs bug as below: BUG: KASAN: slab-use-after-free in sani...
Severity: High
Risk Score: 7.8
EPSS Percentile: 10.5%

CVE-2024-44940

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: fou: remove warn in gue_gro_receive on unsupported protocol Drop the WARN_ON_ONCE inn gue_gro_receive if the encapsulated type is ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.1%

CVE-2024-43900

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: media: xc2028: avoid use-after-free in load_firmware_cb() syzkaller reported use-after-free in load_firmware_cb() [1]. The reason ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 11.0%

CVE-2024-43858

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: jfs: Fix array-index-out-of-bounds in diFree

Severity: High
Risk Score: 7.8
EPSS Percentile: 12.6%

CVE-2024-43839

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: bna: adjust 'name' buf size of bna_tcb and bna_ccb structures To have enough space to write all possible sprintf() args. Currently...
Severity: High
Risk Score: 7.8
EPSS Percentile: 17.3%

CVE-2024-42302

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: PCI/DPC: Fix use-after-free on concurrent DPC and hot-removal Keith reports a use-after-free when a DPC event occurs concurrently ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 12.6%

CVE-2024-42301

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: dev/parport: fix the array out-of-bounds risk Fixed array out-of-bounds issues caused by sprintf by replacing it with snprintf for...
Severity: High
Risk Score: 7.8
EPSS Percentile: 12.6%

CVE-2024-42280

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: mISDN: Fix a use after free in hfcmulti_tx() Don't dereference *sp after calling dev_kfree_skb(*sp).
Severity: High
Risk Score: 7.8
EPSS Percentile: 14.9%

CVE-2024-42271

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net/iucv: fix use after free in iucv_sock_close() iucv_sever_path() is called from process context and from bh context. iucv->path...
Severity: High
Risk Score: 7.8
EPSS Percentile: 15.1%

CVE-2024-42160

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: f2fs: check validation of fault attrs in f2fs_build_fault_attr() - It missed to check validation of fault attrs in parse_options()...
Severity: High
Risk Score: 7.8
EPSS Percentile: 10.1%

CVE-2024-42159

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: scsi: mpi3mr: Sanitise num_phys Information is stored in mr_sas_port->phy_mask, values larger then size of this field shouldn't be...
Severity: High
Risk Score: 7.8
EPSS Percentile: 11.0%

CVE-2024-42148

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: bnx2x: Fix multiple UBSAN array-index-out-of-bounds Fix UBSAN warnings that occur when using a system with 32 physical cpu cores o...
Severity: High
Risk Score: 7.8
EPSS Percentile: 14.9%

CVE-2024-42147

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: crypto: hisilicon/debugfs - Fix debugfs uninit process issue During the zip probe process, the debugfs failure does not stop the p...

Severity: High
Risk Score: 7.8
EPSS Percentile: 11.0%

CVE-2024-42136

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: cdrom: rearrange last_media_change check to avoid unintentional overflow When running syzkaller with the newly reintroduced signed...
Severity: High
Risk Score: 7.8
EPSS Percentile: 11.0%

CVE-2024-42104

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: nilfs2: add missing check for inode numbers on directory entries Syzbot reported that mounting and unmounting a specific pattern o...
Severity: High
Risk Score: 7.8
EPSS Percentile: 10.3%

CVE-2024-41073

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: nvme: avoid double free special payload If a discard request needs to be retried, and that retry may fail before a new special pay...
Severity: High
Risk Score: 7.8
EPSS Percentile: 10.5%

CVE-2024-41070

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: KVM: PPC: Book3S HV: Prevent UAF in kvm_spapr_tce_attach_iommu_group() Al reported a possible use-after-free (UAF) in kvm_spapr_tc...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.5%

CVE-2024-41061

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix array-index-out-of-bounds in dml2/FCLKChangeSupport [Why] Potential out of bounds access in dml2_calculate_rq...
Severity: High
Risk Score: 7.8
EPSS Percentile: 11.0%

CVE-2024-41046

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net: ethernet: lantiq_etop: fix double free in detach The number of the currently released descriptor is never incremented which r...
Severity: High
Risk Score: 7.8
EPSS Percentile: 14.9%

CVE-2024-41000

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: block/ioctl: prefer different overflow check Running syzkaller with the newly reintroduced signed integer overflow sanitizer shows...
Severity: High
Risk Score: 7.8
EPSS Percentile: 13.8%

CVE-2024-40902

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: jfs: xattr: fix buffer overflow for invalid xattr When an xattr size is not what is expected, it is printed out to the kernel log ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.3%

CVE-2024-39496

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: btrfs: zoned: fix use-after-free

due to race with dev replace While loading a zone's info during creation of a block group, we can...
Severity: High
Risk Score: 7.8
EPSS Percentile: 10.7%

CVE-2024-39495

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: greybus: Fix use-after-free bug in gb_interface_release due to race condition. In gb_interface_create, &intf-;>mode_switch_completi...
Severity: High
Risk Score: 7.8
EPSS Percentile: 13.4%

CVE-2024-39494

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ima: Fix use-after-free on a dentry's dname.name ->d_name.name can change on rename and the earlier value can be freed; there are ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 9.9%

CVE-2024-39291

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix buffer size in gfx_v9_4_3_init_ cp_compute_microcode() and rlc_microcode() The function gfx_v9_4_3_init_microcode ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 4.9%

CVE-2024-39277

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: dma-mapping: benchmark: handle NUMA_NO_NODE correctly cpumask_of_node() can be called for NUMA_NO_NODE inside do_map_benchmark() r...
Severity: High
Risk Score: 7.8
EPSS Percentile: 33.6%

CVE-2024-38667

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: riscv: prevent pt_regs corruption for secondary idle threads Top of the kernel thread stack should be reserved for pt_regs. Howeve...
Severity: High
Risk Score: 7.8
EPSS Percentile: 13.5%

CVE-2024-38664

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm: zynqmp_dpsub: Always register bridge We must always register the DRM bridge, since zynqmp_dp_hpd_work_func calls drm_bridge_h...
Severity: High
Risk Score: 7.8
EPSS Percentile: 0.9%

CVE-2024-38630

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: watchdog: cpu5wdt.c: Fix use-after-free bug caused by cpu5wdt_trigger When the cpu5wdt module is removing, the origin code uses de...
Severity: High
Risk Score: 7.8
EPSS Percentile: 14.9%

CVE-2024-38588

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ftrace: Fix possible use-after-free issue in ftrace_location() KASAN reports a bug: BUG: KASAN: use-after-free in ftrace_locati...
Severity: High
Risk Score: 7.8
EPSS Percentile: 15.1%

CVE-2024-38583

Unreachable

Component: Linux
Version: 3.10.108

Description: In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix use-after-free of timer for log writer thread Patch series "nilfs2: fix log writer related issues". This bug fix seri...
Severity: High
Risk Score: 7.8
EPSS Percentile: 14.0%

CVE-2024-38570

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: gfs2: Fix potential glock use-after-free on unmount When a DLM lockspace is released and there ares still locks in that lockspace,...
Severity: High
Risk Score: 7.8
EPSS Percentile: 16.5%

CVE-2024-36921

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mvm: guard against invalid STA ID on removal Guard against invalid station IDs in iwl_mvm_mld_rm_sta_id as that wou...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.8%

CVE-2024-35929

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: rcu/nocb: Fix WARN_ON_ONCE() in the rcu_nocb_bypass_lock() For the kernels built with CONFIG_RCU_NOCB_CPU_DEFAULT_ALL=y and CONFIG...
Severity: High
Risk Score: 7.8
EPSS Percentile: 0.2%

CVE-2024-35887

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ax25: fix use-after-free bugs caused by ax25_ds_del_timer When the ax25 device is detaching, the ax25_dev_device_down() calls ax25...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.9%

CVE-2024-35868

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: smb: client: fix potential UAF in cifs_stats_proc_write() Skip sessions that are being teared down (status == SES_EXITING) to avoi...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.9%

CVE-2024-35867

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: smb: client: fix potential UAF in cifs_stats_proc_show() Skip sessions that are being teared down (status == SES_EXITING) to avoid...
Severity: High
Risk Score: 7.8
EPSS Percentile: 0.6%

CVE-2024-35866

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: smb: client: fix potential UAF in cifs_dump_full_key() Skip sessions that are being teared down (status == SES_EXITING) to avoid U...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.3%

CVE-2024-35864

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: smb: client: fix potential UAF in smb2_is_valid_lease_break() Skip sessions that are being teared down (status == SES_EXITING) to ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.4%

CVE-2024-35863

Unreachable

Component: Linux
Version: 3.10.108

Description: In the Linux kernel, the following vulnerability has been resolved: smb: client: fix potential UAF in is_valid_oplock_break() Skip sessions that are being teared down (status == SES_EXITING) to avoi...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.3%

CVE-2024-35862

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: smb: client: fix potential UAF in smb2_is_network_name_deleted() Skip sessions that are being teared down (status == SES_EXITING) ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.3%

CVE-2024-35861

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: smb: client: fix potential UAF in cifs_signal_cifsd_for_reconnect() Skip sessions that are being teared down (status == SES_EXITIN...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.3%

CVE-2024-27043

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: media: edia: dvbdev: fix a use-after-free In dvb_register_device, *pdvbdev is set equal to dvbdev, which is freed in several error...
Severity: High
Risk Score: 7.8
EPSS Percentile: 0.9%

CVE-2024-27008

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm: nv04: Fix out of bounds access When Output Resource (dcb->or) value is assigned in fabricate_dcb_output(), there may be out o...
Severity: High
Risk Score: 7.8

EPSS Percentile: 1.1%

CVE-2024-26996

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_ncm: Fix UAF ncm object at re-bind after usb ep transport error When ncm function is working and then stop usb0 int...
Severity: High
Risk Score: 7.8
EPSS Percentile: 3.9%

CVE-2024-26981

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix OOB in nilfs_set_de_type The size of the nilfs_type_by_mode array in the fs/nilfs2/dir.c file is defined as "S_IFMT >>...
Severity: High
Risk Score: 7.8
EPSS Percentile: 0.9%

CVE-2024-26958

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: nfs: fix UAF in direct writes In production we have been hitting the following warning consistently ------------[cut here]-----...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.2%

CVE-2024-26957

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: s390/zcrypt: fix reference counting on zcrypt card objects Tests with hot-plugging crytpo cards on KVM guests with debug kernel bu...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.5%

CVE-2024-26944

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: btrfs: zoned: fix use-after-free in do_zone_finish() Shinichiro reported the following use-after-free triggered by the device repl...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.2%

CVE-2024-26928

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: smb: client: fix potential UAF in cifs_debug_files_proc_show() Skip sessions that are being teared down (status == SES_EXITING) to...
Severity: High
Risk Score: 7.8
EPSS Percentile: 2.6%

CVE-2024-26907

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: RDMA/mlx5: Fix fortify source warning while accessing Eth segment ------------[cut here]------------ memcpy: detected field-sp...
Severity: High
Risk Score: 7.8
EPSS Percentile: 0.2%

CVE-2024-26898

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: aoe: fix the potential use-after-free problem in aoecmd_cfg_pkts This patch is against CVE-2023-6270. The description of cve is: ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 0.8%

CVE-2024-26882

Reachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net: ip_tunnel: make sure to pull

inner header in ip_tunnel_rcv() Apply the same fix than ones found in : 8d975c15c0cd ("ip6_tunn...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.6%

CVE-2024-26842

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: core: Fix shift issue in ufshcd_clear_cmd() When task_tag >= 32 (in MCQ mode) and sizeof(unsigned int) == 4, 1U << task...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.9%

CVE-2024-26699

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix array-index-out-of-bounds in dcn35_clkmgr [Why] There is a potential memory access violation while iterating ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 9.7%

CVE-2024-26689

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ceph: prevent use-after-free in encode_cap_msg() In fs/ceph/caps.c, in encode_cap_msg(), "use after free" error was caught by KASA...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.3%

CVE-2024-26625

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: llc: call sock_orphan() at release time syzbot reported an interesting trace [1] caused by a stale sk->sk_wq pointer in a closed l...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.1%

CVE-2024-26622

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: tomoyo: fix UAF write bug in tomoyo_write_control() Since tomoyo_write_control() updates head->write_buf when write() of long line...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.2%

CVE-2024-22705

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in ksmbd in the Linux kernel before 6.6.10. smb2_get_data_area_len in fs/smb/server/smb2misc.c can cause an smb_strndup_from_utf16 out-of-bounds access because the relationship...
Severity: High
Risk Score: 7.8
EPSS Percentile: 2.4%

CVE-2024-21803

Unreachable

Component: Linux
Version: 3.10.108
Description: Use After Free vulnerability in Linux Linux kernel kernel on Linux, x86, ARM (bluetooth modules) allows Local Execution of Code. This vulnerability is associated with program files https://gitee.Com/a...
Severity: High
Risk Score: 7.8
EPSS Percentile: 10.7%

CVE-2023-53023

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net: nfc: Fix use-after-free in local_cleanup() Fix a use-after-free that occurs in kfree_skb() called from local_cleanup(). This ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 2.9%

CVE-2023-52988

Unreachable

Component: Linux
Version: 3.10.108

Description: In the Linux kernel, the following vulnerability has been resolved: ALSA: hda/via: Avoid potential array out-of-bound in add_secret_dac_path() snd_hda_get_connections() can return a negative error c...
Severity: High
Risk Score: 7.8
EPSS Percentile: 2.1%

CVE-2023-52975

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: scsi: iscsi_tcp: Fix UAF during logout when accessing the shost ipaddress Bug report and analysis from Ding Hui. During iSCSI ses...
Severity: High
Risk Score: 7.8
EPSS Percentile: 2.7%

CVE-2023-52974

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: scsi: iscsi_tcp: Fix UAF during login when accessing the shost ipaddress If during iscsi_sw_tcp_session_create() iscsi_tcp_r2tpool...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.5%

CVE-2023-52973

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: vc_screen: move load of struct vc_data pointer in vcs_read() to avoid UAF After a call to console_unlock() in vcs_read() the vc_da...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.5%

CVE-2023-52922

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: can: bcm: Fix UAF in bcm_proc_show() BUG: KASAN: slab-use-after-free in bcm_proc_show+0x969/0xa80 Read of size 8 at addr ffff88815...
Severity: High

Risk Score: 7.8
EPSS Percentile: 7.0%

CVE-2023-52921

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix possible UAF in amdgpu_cs_pass1() Since the gang_size check is outside of chunk parsing loop, we need to reset i b...
Severity: High
Risk Score: 7.8
EPSS Percentile: 4.6%

CVE-2023-52818

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd: Fix UBSAN array-index-out-of-bounds for SMU7 For pptable structs that use flexible array sizes, use flexible arrays.
Severity: High
Risk Score: 7.8
EPSS Percentile: 0.9%

CVE-2023-52812

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd: check num of link levels when update pcie param In SR-IOV environment, the value of pcie_table->num_of_link_levels will b...
Severity: High
Risk Score: 7.8
EPSS Percentile: 29.3%

CVE-2023-52805

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: jfs: fix array-index-out-of-bounds in diAlloc Currently there is not check against the agno of the iag while allocating new inodes...
Severity: High
Risk Score: 7.8
EPSS Percentile: 17.2%

CVE-2023-52799

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: jfs: fix array-index-out-of-bounds in dbFindLeaf Currently while searching for dmtree_t for sufficient free blocks there is an arr...
Severity: High
Risk Score: 7.8
EPSS Percentile: 14.1%

CVE-2023-52760

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: gfs2: Fix slab-use-after-free in gfs2_qd_dealloc In gfs2_put_super(), whether withdrawn or not, the quota should be cleaned up by ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.3%

CVE-2023-52757

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: smb: client: fix potential deadlock when releasing mids All release_mid() callers seem to hold a reference of @mid so there is no ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 0.6%

CVE-2023-52752

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: smb: client: fix use-after-free bug in cifs_debug_data_proc_show() Skip SMB sessions that are being teared down (e.g. @ses->ses_st...
Severity: High
Risk Score: 7.8
EPSS Percentile: 0.9%

CVE-2023-52751

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: smb: client: fix use-after-free in smb2_query_info_compound() The following UAF was triggered when running fstests generic/072 wit...
Severity: High

Risk Score: 7.8
EPSS Percentile: 27.9%

CVE-2023-52741

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: cifs: Fix use-after-free in rdata->read_into_pages() When the network status is unstable, use-after-free may occur when read data ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.8%

CVE-2023-52664

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net: atlantic: eliminate double free in error handling logic Driver has a logic leak in ring data allocation/free, where aq_ring_f...
Severity: High
Risk Score: 7.8
EPSS Percentile: 3.9%

CVE-2023-52642

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: media: rc: bpf attach/detach requires write permission Note that bpf attach/detach also requires CAP_NET_ADMIN.
Severity: High
Risk Score: 7.8
EPSS Percentile: 0.9%

CVE-2023-52624

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Wake DMCUB before executing GPINT commands [Why] DMCUB can be in idle when we attempt to interface with the HW th...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.7%

CVE-2023-52621

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: bpf: Check rcu_read_lock_trace_held() before calling bpf map helpers These three bpf_map_{lookup,update,delete}_elem() helpers are...
Severity: High
Risk Score: 7.8
EPSS Percentile: 0.2%

CVE-2023-52614

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: PM / devfreq: Fix buffer overflow in trans_stat_show Fix buffer overflow in trans_stat_show(). Convert simple snprintf to the mor...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.1%

CVE-2023-52604

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: FS:JFS:UBSAN:array-index-out-of-bounds in dbAdjTree Syzkaller reported the following issue: UBSAN: array-index-out-of-bounds in f...
Severity: High
Risk Score: 7.8
EPSS Percentile: 0.8%

CVE-2023-52603

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: UBSAN: array-index-out-of-bounds in dtSplitRoot Syzkaller reported the following issue: oop0: detected capacity change from 0 to ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 2.0%

CVE-2023-52602

Unreachable

Component: Linux
Version: 3.10.108

Description: In the Linux kernel, the following vulnerability has been resolved: jfs: fix slab-out-of-bounds Read in dtSearch Currently while searching for current page in the sorted entry table of the page ther...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.0%

CVE-2023-52601

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: jfs: fix array-index-out-of-bounds in dbAdjTree Currently there is a bound check missing in the dbAdjTree while accessing the dmt_...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.0%

CVE-2023-52600

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: jfs: fix uaf in jfs_evict_inode When the execution of diMount(ipimap) fails, the object ipimap that has been released may be acces...
Severity: High
Risk Score: 7.8
EPSS Percentile: 0.8%

CVE-2023-52599

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: jfs: fix array-index-out-of-bounds in diNewExt [Syz report] UBSAN: array-index-out-of-bounds in fs/jfs/jfs_imap.c:2360:2 index -87...
Severity: High
Risk Score: 7.8
EPSS Percentile: 0.8%

CVE-2023-52594

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: wifi: ath9k: Fix potential array-index-out-of-bounds read in ath9k_htc_txstatus() Fix an array-index-out-of-bounds read in ath9k_h...
Severity: High
Risk Score: 7.8

EPSS Percentile: 1.0%

CVE-2023-52591

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: reiserfs: Avoid touching renamed directory if parent does not change The VFS will not be locking moved directory if its parent doe...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.3%

CVE-2023-52572

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: cifs: Fix UAF in cifs_demultiplex_thread() There is a UAF when xfstests on cifs: BUG: KASAN: use-after-free in smb2_is_network_...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.1%

CVE-2023-52531

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mvm: Fix a memory corruption issue A few lines above, space is kzalloc()'ed for: sizeof(struct iwl_nvm_data) + si...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.7%

CVE-2023-52515

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: RDMA/srp: Do not call scsi_done() from srp_abort() After scmd_eh_abort_handler() has called the SCSI LLD eh_abort_handler callback...
Severity: High
Risk Score: 7.8
EPSS Percentile: 2.6%

CVE-2023-52482

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: x86/srso: Add SRSO mitigation for Hygon processors Add mitigation for the speculative return stack overflow vulnerability which ex...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.1%

CVE-2023-52475

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: Input: powermate - fix use-after-free in powermate_config_complete syzbot has found a use-after-free bug [1] in the powermate driv...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.0%

CVE-2023-52445

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: media: pvrusb2: fix use after free on context disconnection Upon module load, a kthread is created targeting the pvr2_context_thre...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.0%

CVE-2023-52436

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: f2fs: explicitly null-terminate the xattr list When setting an xattr, explicitly null-terminate the xattr list. This eliminates t...
Severity: High
Risk Score: 7.8
EPSS Percentile: 0.8%

CVE-2023-51042

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 6.4.12, amdgpu_cs_wait_all_fences in drivers/gpu/drm/amd/amdgpu/amdgpu_cs.c has a fence use-after-free.
Severity: High

Risk Score: 7.8
EPSS Percentile: 2.3%

CVE-2023-4921 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: A use-after-free vulnerability in the Linux kernel's net/sched: sch_qfq component can be exploited to achieve local privilege escalation. When the plug qdisc is used as a class of the qfq qdisc, send...
Severity: High
Risk Score: 7.8
EPSS Percentile: 19.5%

CVE-2023-4623 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A use-after-free vulnerability in the Linux kernel's net/sched: sch_hfsc (HFSC qdisc traffic control) component can be exploited to achieve local privilege escalation. If a class with a link-sharing ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 2.2%

CVE-2023-40283

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in l2cap_sock_release in net/bluetooth/l2cap_sock.c in the Linux kernel before 6.4.10. There is a use-after-free because the children of an sk are mishandled.
Severity: High
Risk Score: 7.8
EPSS Percentile: 0.8%

CVE-2023-3776 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A use-after-free vulnerability in the Linux kernel's net/sched: cls_fw component can be exploited to achieve local privilege escalation. If tcf_change_indev() fails, fw_set_parms() will immediately r...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.8%

CVE-2023-3611 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An out-of-bounds write vulnerability in the Linux kernel's net/sched: sch_qfq component can be exploited to achieve local privilege escalation. The qfq_change_agg() function in net/sched/sch_qfq.c al...
Severity: High
Risk Score: 7.8
EPSS Percentile: 2.0%

CVE-2023-31436 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: qfq_change_class in net/sched/sch_qfq.c in the Linux kernel before 6.2.13 allows an out-of-bounds write because lmax can exceed QFQ_MIN_LMAX.
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.6%

CVE-2023-3111

Unreachable

Component: Linux
Version: 3.10.108
Description: A use after free vulnerability was found in prepare_to_relocate in fs/btrfs/relocation.c in btrfs in the Linux Kernel. This possible flaw can be triggered by calling btrfs_ioctl_balance() before calli...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.7%

CVE-2023-26242

Unreachable

Component: Linux
Version: 3.10.108
Description: afu_mmio_region_get_by_offset in drivers/fpga/dfl-afu-region.c in the Linux kernel through 6.1.12 has an integer overflow.
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.4%

CVE-2023-23559

Component: Linux
Version: 3.10.108
Description: In rndis_query_oid in drivers/net/wireless/rndis_wlan.c in the Linux kernel through 6.1.5, there is an integer overflow in an addition.
Severity: High
Risk Score: 7.8
EPSS Percentile: 3.9%

CVE-2023-22995

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 5.17, an error path in dwc3_qcom_acpi_register_core in drivers/usb/dwc3/dwc3-qcom.c lacks certain platform_device_put and kfree calls.
Severity: High
Risk Score: 7.8
EPSS Percentile: 0.8%

CVE-2023-2124 🔥 PoC

Component: Linux
Version: 3.10.108
Description: An out-of-bounds memory access flaw was found in the Linux kernel's XFS file system in how a user restores an XFS image after failure (with a dirty log journal). This flaw allows a local user to crash...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.1%

CVE-2023-2008 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A flaw was found in the Linux kernel's udmabuf device driver. The specific flaw exists within a fault handler. The issue results from the lack of proper validation of user-supplied data, which can res...
Severity: High
Risk Score: 7.8
EPSS Percentile: 73.0%

CVE-2023-2007

Component: Linux
Version: 3.10.108
Description: The specific flaw exists within the DPT I2O Controller driver. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this in conjunction w...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.1%

CVE-2023-1829 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A use-after-free vulnerability in the Linux Kernel traffic control index filter (tcindex) can be exploited to achieve local privilege escalation. The tcindex_delete function which does not properly de...
Severity: High
Risk Score: 7.8
EPSS Percentile: 39.3%

CVE-2023-1670

Component: Linux
Version: 3.10.108
Description: A flaw use after free in the Linux kernel Xircom 16-bit PCMCIA (PC-card) Ethernet driver was found.A local user could use this flaw to crash the system or potentially escalate their privileges on the ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 13.9%

CVE-2023-1118

Component: Linux
Version: 3.10.108
Description: A flaw use after free in the Linux kernel integrated infrared receiver/transceiver driver was found in the way user detaching rc device. A local user could use this flaw to crash the system or potenti...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.6%

CVE-2023-0240

Component: Linux
Version: 3.10.108
Description: There is a logic error in io_uring's implementation which can be used to trigger a use-after-free vulnerability leading to privilege escalation. In the io_prep_async_work function the assumption that...
Severity: High
Risk Score: 7.8
EPSS Percentile: 3.3%

CVE-2023-0030

Component: Linux
Version: 3.10.108
Description: A use-after-free flaw was found in the Linux kernel's nouveau driver in how a user triggers a memory overflow that causes the nvkm_vma_tail function to fail. This flaw allows a local user to crash or ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 4.2%

CVE-2022-49761

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: btrfs: always report error in run_one_delayed_ref() Currently we have a btrfs_debug() for run_one_delayed_ref() failure, but if en...
Severity: High
Risk Score: 7.8
EPSS Percentile: 2.1%

CVE-2022-49755

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f_fs: Prevent race during ffs_ep0_queue_wait While performing fast composition switch, there is a possibility that th...
Severity: High
Risk Score: 7.8
EPSS Percentile: 2.2%

CVE-2022-49730

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Resolve NULL ptr dereference after an ELS LOGO is aborted A use-after-free crash can occur after an ELS LOGO is aborte...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.2%

CVE-2022-49700

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: mm/slub: add missing TID updates on slab deactivation The fastpath in slab_alloc_node() assumes that c->slab is stable as long as ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 20.1%

CVE-2022-49685

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: iio: trigger: sysfs: fix use-after-free on remove Ensure that the irq_work has completed before the trigger is freed. ==========...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.5%

CVE-2022-49651

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: srcu: Tighten

cleanup_srcu_struct() GP checks Currently, cleanup_srcu_struct() checks for a grace period in progress, but it does ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.7%

CVE-2022-49622

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: avoid skb access on nf_stolen When verdict is NF_STOLEN, the skb might have been freed. When tracing is ena...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.7%

CVE-2022-49541

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: cifs: fix potential double free during failed mount RHBZ: https://bugzilla.redhat.com/show_bug.cgi?id=2088799
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.5%

CVE-2022-49535

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Fix null pointer dereference after failing to issue FLOGI and PLOGI If lpfc_issue_els_flogi() fails and returns non-ze...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.2%

CVE-2022-49530

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd/pm: fix double free in si_parse_power_table() In function si_parse_power_table(), array adev->pm.dpm.ps and its member is ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.9%

CVE-2022-49524

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: media: pci: cx23885: Fix the error handling in cx23885_initdev() When the driver fails to call the dma_set_mask(), the driver will...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.5%

CVE-2022-49501

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: usbnet: Run unregister_netdev() before unbind() again Commit 2c9d6c2b871d ("usbnet: run unbind() before unregister_netdev()") soug...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.5%

CVE-2022-49493

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ASoC: rt5645: Fix errorenous cleanup order There is a logic error when removing rt5645 device as the function rt5645_i2c_remove() ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.9%

CVE-2022-49478

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: media: pvrusb2: fix array-index-out-of-bounds in pvr2_i2c_core_init Syzbot reported that -1 is used as array index. The problem wa...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.9%

CVE-2022-49471

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: rtw89: cfo: check mac_id to avoid out-of-bounds Somehow, hardware reports incorrect mac_id and pollute memory. Check index before ...
Severity: High

Risk Score: 7.8
EPSS Percentile: 6.2%

CVE-2022-49465

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: blk-throttle: Set BIO_THROTTLED when bio has been throttled 1.In current process, all bio will set the BIO_THROTTLED flag after __...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.2%

CVE-2022-49412

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: bfq: Avoid merging queues with different parents It can happen that the parent of a bfqq changes between the moment we decide two ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.5%

CVE-2022-49385

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: driver: base: fix UAF when driver_attach failed When driver_attach(drv); failed, the driver_private will be freed. But it has been...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.5%

CVE-2022-49349

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ext4: fix use-after-free in ext4_rename_dir_prepare We got issue as follows: EXT4-fs (loop0): mounted filesystem without journal. ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.9%

CVE-2022-49328

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: mt76: fix use-after-free by removing a non-RCU wcid pointer Fixes an issue caught by KASAN about use-after-free in mt76_txq_schedu...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.4%

CVE-2022-49291

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ALSA: pcm: Fix races among concurrent hw_params and hw_free calls Currently we have neither proper check nor protection against th...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.5%

CVE-2022-49288

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ALSA: pcm: Fix races among concurrent prealloc proc writes We have no protection against concurrent PCM buffer preallocation chang...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.5%

CVE-2022-49179

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: block, bfq: don't move oom_bfqq Our test report a UAF: [2073.019181] ==========...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.5%

CVE-2022-49176

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: bfq: fix use-after-free in

bfq_dispatch_request KASAN reports a use-after-free report when doing normal scsi-mq test [69832.23903...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.5%

CVE-2022-49168

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: btrfs: do not clean up repair bio if submit fails The submit helper will always run bio_endio() on the bio if it fails to submit, ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.4%

CVE-2022-49114

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: scsi: libfc: Fix use after free in fc_exch_abts_resp() fc_exch_release(ep) will decrease the ep's reference count. When the refere...
Severity: High
Risk Score: 7.8
EPSS Percentile: 20.6%

CVE-2022-49111

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: Bluetooth: Fix use after free in hci_send_acl This fixes the following trace caused by receiving HCI_EV_DISCONN_PHY_LINK_COMPLETE ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 19.2%

CVE-2022-49078

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: lz4: fix LZ4_decompress_safe_partial read out of bound When partialDecoding, it is EOF if we've either filled the output buffer or...
Severity: High
Risk Score: 7.8
EPSS Percentile: 22.4%

CVE-2022-49059

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: nfc: nci: add flush_workqueue to prevent uaf Our detector found a concurrent use-after-free bug when detaching an NCI device. The ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 2.8%

CVE-2022-49058

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: cifs: potential buffer overflow in handling symlinks Smatch printed a warning: arch/x86/crypto/poly1305_glue.c:198 poly1305_updat...
Severity: High
Risk Score: 7.8
EPSS Percentile: 20.1%

CVE-2022-49053

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: scsi: target: tcmu: Fix possible page UAF tcmu_try_get_data_page() looks up pages under cmdr_lock, but it does not take refcount p...
Severity: High
Risk Score: 7.8
EPSS Percentile: 22.4%

CVE-2022-49029

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: hwmon: (ibmpex) Fix possible UAF when ibmpex_register_bmc() fails Smatch report warning as follows: drivers/hwmon/ibmpex.c:509 ib...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.7%

CVE-2022-49006

Unreachable

Component: Linux
Version: 3.10.108

Description: In the Linux kernel, the following vulnerability has been resolved: tracing: Free buffers when a used dynamic event is removed After 65536 dynamic events have been added and removed, the "type" fiel...
Severity: High
Risk Score: 7.8
EPSS Percentile: 30.2%

CVE-2022-48990

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix use-after-free during gpu recovery [Why] [754.862560] refcount_t: underflow; use-after-free. [754.8628...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.7%

CVE-2022-48951

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ASoC: ops: Check bounds for second channel in snd_soc_put_volsw_sx() The bounds checks in snd_soc_put_volsw_sx() are only being ap...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.7%

CVE-2022-48950

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: perf: Fix perf_pending_task() UaF Per syzbot it is possible for perf_pending_task() to run after the event is free()'d. There are ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 20.4%

CVE-2022-48948

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: usb: gadget: uvc: Prevent buffer overflow in setup handler Setup function uvc_function_setup permits control transfer requests wit...
Severity: High
Risk Score: 7.8

EPSS Percentile: 7.6%

CVE-2022-48943

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: KVM: x86/mmu: make apf token non-zero to fix bug In current async pagefault logic, when a page is ready, KVM relies on kvm_arch_ca...
Severity: High
Risk Score: 7.8
EPSS Percentile: 14.5%

CVE-2022-48919

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: cifs: fix double free race when mount fails in cifs_get_root() When cifs_get_root() fails during cifs_smb3_do_mount() we call deac...
Severity: High
Risk Score: 7.8
EPSS Percentile: 8.4%

CVE-2022-48805

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net: usb: ax88179_178a: Fix out-of-bounds accesses in RX fixup ax88179_rx_fixup() contains several out-of-bounds accesses that can...
Severity: High
Risk Score: 7.8
EPSS Percentile: 17.6%

CVE-2022-48792

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: scsi: pm8001: Fix use-after-free for aborted SSP/STP sas_task Currently a use-after-free may occur if a sas_task is aborted by the...
Severity: High
Risk Score: 7.8
EPSS Percentile: 11.0%

CVE-2022-48791

Unreachable

Component: Linux
Version: 3.10.108

Description: In the Linux kernel, the following vulnerability has been resolved: scsi: pm8001: Fix use-after-free for aborted TMF sas_task Currently a use-after-free may occur if a TMF sas_task is aborted before...
Severity: High
Risk Score: 7.8
EPSS Percentile: 11.0%

CVE-2022-48789

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: nvme-tcp: fix possible use-after-free in transport error_recovery work While nvme_tcp_submit_async_event_work is checking the ctrl...
Severity: High
Risk Score: 7.8
EPSS Percentile: 23.0%

CVE-2022-48788

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: nvme-rdma: fix possible use-after-free in transport error_recovery work While nvme_rdma_submit_async_event_work is checking the ct...
Severity: High
Risk Score: 7.8
EPSS Percentile: 10.5%

CVE-2022-48733

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: btrfs: fix use-after-free after failure to create a snapshot At ioctl.c:create_snapshot(), we allocate a pending snapshot structur...
Severity: High
Risk Score: 7.8
EPSS Percentile: 10.7%

CVE-2022-48702

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ALSA: emu10k1: Fix out of bounds access in snd_emu10k1_pcm_channel_alloc() The voice allocator sometimes begins allocating from ne...
Severity: High
Risk Score: 7.8

EPSS Percentile: 1.7%

CVE-2022-48695

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: scsi: mpt3sas: Fix use-after-free warning Fix the following use-after-free warning which is observed during controller reset: ref...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.4%

CVE-2022-48423

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 6.1.3, fs/ntfs3/record.c does not validate resident attribute names. An out-of-bounds write may occur.
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.8%

CVE-2022-45934

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 6.0.10. l2cap_config_req in net/bluetooth/l2cap_core.c has an integer wraparound via L2CAP_CONF_REQ packets.
Severity: High
Risk Score: 7.8
EPSS Percentile: 53.6%

CVE-2022-4095

Component: Linux
Version: 3.10.108
Description: A use-after-free flaw was found in Linux kernel before 5.19.2. This issue occurs in cmd_hdl_filter in drivers/staging/rtl8712/rtl8712_cmd.c, allowing an attacker to launch a local denial of service at...
Severity: High
Risk Score: 7.8
EPSS Percentile: 2.2%

CVE-2022-36123 🔥 PoC

Component: Linux
Version: 3.10.108

Description: The Linux kernel before 5.18.13 lacks a certain clear operation for the block starting symbol (.bss). This allows Xen PV guest OS users to cause a denial of service or gain privileges.
Severity: High
Risk Score: 7.8
EPSS Percentile: 42.5%

CVE-2022-3565

Unreachable

Component: Linux
Version: 3.10.108
Description: A vulnerability, which was classified as critical, has been found in Linux Kernel. Affected by this issue is the function del_timer of the file drivers/isdn/mISDN/l1oip_core.c of the component Bluetoo...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.0%

CVE-2022-3424

Component: Linux
Version: 3.10.108
Description: A use-after-free flaw was found in the Linux kernel's SGI GRU driver in the way the first gru_file_unlocked_ioctl function is called by the user, where a fail pass occurs in the gru_check_chiplet_assi...
Severity: High
Risk Score: 7.8
EPSS Percentile: 4.1%

CVE-2022-32981 🔥 PoC

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 5.18.3 on powerpc 32-bit platforms. There is a buffer overflow in ptrace PEEKUSER and POKEUSER (aka PEEKUSR and POKEUSR) when accessing floating poi...
Severity: High
Risk Score: 7.8
EPSS Percentile: 62.2%

CVE-2022-30594 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The Linux kernel before 5.17.2 mishandles seccomp permissions. The PTRACE_SEIZE code path allows attackers to bypass intended restrictions on setting the PT_SUSPEND_SECCOMP flag.
Severity: High
Risk Score: 7.8
EPSS Percentile: 45.3%

CVE-2022-29968

Component: Linux
Version: 3.10.108

Description: An issue was discovered in the Linux kernel through 5.17.5. io_rw_init_file in fs/io_uring.c lacks initialization of kiocb->private.
Severity: High
Risk Score: 7.8
EPSS Percentile: 77.5%

CVE-2022-2978

Component: Linux
Version: 3.10.108
Description: A flaw use after free in the Linux kernel NILFS file system was found in the way user triggers function security_inode_alloc to fail with following call to function nilfs_mdt_destroy. A local user cou...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.9%

CVE-2022-28390

Unreachable

Component: Linux
Version: 3.10.108
Description: ems_usb_start_xmit in drivers/net/can/usb/ems_usb.c in the Linux kernel through 5.17.1 has a double free.
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.5%

CVE-2022-27666 🔥 Commercial Exploit

Reachable

Component: Linux
Version: 3.10.108
Description: A heap buffer overflow flaw was found in IPsec ESP transformation code in net/ipv4/esp4.c and net/ipv6/esp6.c. This flaw allows a local attacker with a normal user privilege to overwrite kernel heap o...
Severity: High
Risk Score: 7.8
EPSS Percentile: 77.1%

CVE-2022-26490

Unreachable

Component: Linux
Version: 3.10.108
Description: st21nfca_connectivity_event_received in drivers/nfc/st21nfca/se.c in the Linux kernel through 5.16.12 has EVT_TRANSACTION buffer overflows because of untrusted length parameters.
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.2%

CVE-2022-2588 🔥 Commercial Exploit

Component: Linux
Version: 3.10.108
Description: It was discovered that the cls_route filter implementation in the Linux kernel would not remove an old filter from the hashtable before freeing it if its handle had the value 0.
Severity: High
Risk Score: 7.8
EPSS Percentile: 98.7%

CVE-2022-2586 🔥 In VulnCheck KEV

Component: Linux
Version: 3.10.108
Description: It was discovered that a nft object or expression could reference a nft set on a different nft table, leading to a use-after-free once that table was deleted.
Severity: High
Risk Score: 7.8
EPSS Percentile: 80.4%

CVE-2022-25265 🔥 PoC

Component: Linux
Version: 3.10.108
Description: In the Linux kernel through 5.16.10, certain binary files may have the exec-all attribute if they were built in approximately 2003 (e.g., with GCC 3.2.2 and Linux kernel 2.4.20). This can cause execut...
Severity: High
Risk Score: 7.8
EPSS Percentile: 45.3%

CVE-2022-24958

Unreachable

Component: Linux
Version: 3.10.108
Description: drivers/usb/gadget/legacy/inode.c in the Linux kernel through 5.16.8 mishandles dev->buf release.
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.3%

CVE-2022-1679

Component: Linux
Version: 3.10.108
Description: A use-after-free flaw was found in the Linux kernel's Atheros wireless adapter driver in the way a user forces the ath9k_htc_wait_for_target function to fail with some input messages. This flaw allows...
Severity: High
Risk Score: 7.8
EPSS Percentile: 27.3%

CVE-2022-1652

Component: Linux
Version: 3.10.108
Description: Linux Kernel could allow a local attacker to execute arbitrary code on the system, caused by a concurrency use-after-free flaw in the bad_flp_intr function. By executing a specially-crafted program, a...
Severity: High
Risk Score: 7.8
EPSS Percentile: 44.0%

CVE-2022-1419

Component: Linux
Version: 3.10.108
Description: The root cause of this vulnerability is that the ioctl$DRM_IOCTL_MODE_DESTROY_DUMB can decrease refcount of *drm_vgem_gem_object *(created in *vgem_gem_dumb_create*) concurrently, and *vgem_gem_dumb_c...
Severity: High
Risk Score: 7.8
EPSS Percentile: 2.2%

CVE-2022-1011 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A use-after-free flaw was found in the Linux kernel's FUSE filesystem in the way a user triggers write(). This flaw allows a local user to gain unauthorized access to data from the FUSE filesystem, re...
Severity: High
Risk Score: 7.8
EPSS Percentile: 34.9%

CVE-2022-0516

Component: Linux
Version: 3.10.108
Description: A vulnerability was found in kvm_s390_guest_sida_op in the arch/s390/kvm/kvm-s390.c function in KVM for s390 in the Linux kernel. This flaw allows a local attacker with a normal user privilege to obta...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.6%

CVE-2022-0492 🔥 Weaponized

Unreachable

Component: Linux
Version: 3.10.108
Description: A vulnerability was found in the Linux kernel's cgroup_release_agent_write in the kernel/cgroup/cgroup-v1.c function. This flaw, under certain circumstances, allows the use of the cgroups v1 release_a...
Severity: High
Risk Score: 7.8
EPSS Percentile: 94.8%

CVE-2022-0330

Component: Linux
Version: 3.10.108
Description: A random memory access flaw was found in the Linux kernel's GPU i915 kernel driver functionality in the way a user may run malicious code on the GPU. This flaw allows a local user to crash the system ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 14.0%

CVE-2021-47656

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: jffs2: fix use-after-free in jffs2_clear_xattr_subsystem When we mount a jffs2 image, assume that the first few blocks of the imag...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.9%

CVE-2021-47646

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: Revert "Revert "block, bfq: honor already-setup queue merges"" A crash [1] happened to be triggered in conjunction with commit 2d5...
Severity: High
Risk Score: 7.8
EPSS Percentile: 22.4%

CVE-2021-47634

Reachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ubi: Fix race condition between ctrl_cdev_ioctl and ubi_cdev_ioctl Hulk Robot reported a KASAN report about use-after-free: =====...
Severity: High
Risk Score: 7.8
EPSS Percentile: 25.5%

CVE-2021-47600

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: dm btree remove: fix use after free in rebalance_children() Move dm_tm_unlock() after dm_tm_dec().

Severity: High
Risk Score: 7.8
EPSS Percentile: 10.5%

CVE-2021-47589

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: igbvf: fix double free in `igbvf_probe` In `igbvf_probe`, if register_netdev() fails, the program will go to label err_hw_init, an...
Severity: High
Risk Score: 7.8
EPSS Percentile: 17.6%

CVE-2021-47576

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: scsi: scsi_debug: Sanity check block descriptor length in resp_mode_select() In resp_mode_select() sanity check the block descript...
Severity: High
Risk Score: 7.8
EPSS Percentile: 10.5%

CVE-2021-47571

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: staging: rtl8192e: Fix use after free in _rtl92e_pci_disconnect() The free_rtllib() function frees the "dev" pointer so there is u...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.8%

CVE-2021-47549

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: sata_fsl: fix UAF in sata_fsl_port_stop when rmmod sata_fsl When the `rmmod sata_fsl.ko` command is executed in the PPC64 GNU/Linu...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.7%

CVE-2021-47521

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: can: sja1000: fix use after free in ems_pcmcia_add_card() If the last channel is not available then "dev" is freed. Fortunately, ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.7%

CVE-2021-47520

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: can: pch_can: pch_can_rx_normal: fix use after free After calling netif_receive_skb(skb), dereferencing skb is unsafe. Especially,...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.7%

CVE-2021-47506

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: nfsd: fix use-after-free due to delegation race A delegation break could arrive as soon as we've called vfs_setlease. A delegatio...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.2%

CVE-2021-47485

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: IB/qib: Protect from buffer overflow in struct qib_user_sdma_pkt fields Overflowing either addrlimit or bytes_togo can allow users...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.5%

CVE-2021-47404

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: HID: betop: fix slab-out-of-bounds Write in betop_probe Syzbot reported slab-out-of-bounds Write bug in hid-betopff driver.

The pr...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.0%

CVE-2021-47386

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: hwmon: (w83791d) Fix NULL pointer dereference by removing unnecessary structure field If driver read val value sufficient for (val...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.5%

CVE-2021-47379

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: blk-cgroup: fix UAF by grabbing blkcg lock before destroying blkg pd KASAN reports a use-after-free report when doing fuzz test: ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.6%

CVE-2021-47372

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net: macb: fix use after free on rmmod plat_dev->dev->platform_data is released by platform_device_unregister(), use of pclk and h...
Severity: High
Risk Score: 7.8
EPSS Percentile: 0.9%

CVE-2021-47357

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: atm: iphase: fix possible use-after-free in ia_module_exit() This module's remove path calls del_timer(). However, that function d...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.0%

CVE-2021-47355

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: atm: nicstar: Fix possible use-after-free in nicstar_cleanup() This module's remove path calls del_timer(). However, that function...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.4%

CVE-2021-47352

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: virtio-net: Add validation for used length This adds validation for used length (might come from an untrusted device) to avoid dat...
Severity: High
Risk Score: 7.8
EPSS Percentile: 4.2%

CVE-2021-47342

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ext4: fix possible UAF when remounting r/o a mmp-protected file system After commit 618f003199c6 ("ext4: fix memory leak in ext4_f...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.7%

CVE-2021-47336

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: smackfs: restrict bytes count in smk_set_cipso() Oops, I failed to update subject line. From 07571157c91b98ce1a4aa70967531e64b78e...
Severity: High
Risk Score: 7.8
EPSS Percentile: 3.2%

CVE-2021-47334

Unreachable

Component: Linux
Version: 3.10.108

Description: In the Linux kernel, the following vulnerability has been resolved: misc/libmasm/module: Fix two use after free in ibmasm_init_one In ibmasm_init_one, it calls ibmasm_init_remote_input_dev(). Inside...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.5%

CVE-2021-47328

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: scsi: iscsi: Fix conn use after free during resets If we haven't done a unbind target call we can race where iscsi_conn_teardown w...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.3%

CVE-2021-47321

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: watchdog: Fix possible use-after-free by calling del_timer_sync() This driver's remove path calls del_timer(). However, that funct...
Severity: High
Risk Score: 7.8
EPSS Percentile: 0.7%

CVE-2021-47310

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net: ti: fix UAF in tlan_remove_one priv is netdev private data and it cannot be used after free_netdev() call. Using priv after f...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.0%

CVE-2021-47254

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: gfs2: Fix use-after-free in gfs2_glock_shrink_scan The GLF_LRU flag is checked under lru_lock in gfs2_glock_remove_from_lru() to r...
Severity: High
Risk Score: 7.8

EPSS Percentile: 1.4%

CVE-2021-47194

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: cfg80211: call cfg80211_stop_ap when switch from P2P_GO type If the userspace tools switch from NL80211_IFTYPE_P2P_GO to NL80211_I...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.7%

CVE-2021-47118

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: pid: take a reference when initializing `cad_pid` During boot, kernel_init_freeable() initializes `cad_pid` to the init task's str...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.2%

CVE-2021-47103 🔥 PoC

Reachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: inet: fully convert sk->sk_rx_dst to RCU rules syzbot reported various issues around early demux, one being included in this chang...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.1%

CVE-2021-47082

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: tun: avoid double free in tun_free_netdev Avoid double free in tun_free_netdev() by moving the dev->tstats and tun->security alloc...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.9%

CVE-2021-46936

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net: fix use-after-free in tw_timer_handler A real world panic issue was found as follow in Linux 5.4. BUG: unable to handle ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 1.2%

CVE-2021-45469 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In __f2fs_setxattr in fs/f2fs/xattr.c in the Linux kernel through 5.15.11, there is an out-of-bounds memory access when an inode has an invalid last xattr entry.
Severity: High
Risk Score: 7.8
EPSS Percentile: 37.4%

CVE-2021-4439

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: isdn: cpai: check ctr->cnr to avoid array index out of bound The cmtp_add_connection() would add a cmtp session to a controller an...
Severity: High
Risk Score: 7.8
EPSS Percentile: 10.5%

CVE-2021-42252

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in aspeed_lpc_ctrl_mmap in drivers/soc/aspeed/aspeed-lpc-ctrl.c in the Linux kernel before 5.14.6. Local attackers able to access the Aspeed LPC control interface could overwri...
Severity: High
Risk Score: 7.8
EPSS Percentile: 18.5%

CVE-2021-42008 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The decode_data function in drivers/net/hamradio/6pack.c in the Linux kernel before 5.13.13 has a

slab out-of-bounds write. Input from a process that has the CAP_NET_ADMIN capability can lead to root ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 73.2%

CVE-2021-41864

Unreachable

Component: Linux
Version: 3.10.108
Description: prealloc_elems_and_freelist in kernel/bpf/stackmap.c in the Linux kernel before 5.14.12 allows unprivileged users to trigger an eBPF multiplication integer overflow with a resultant out-of-bounds writ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 5.6%

CVE-2021-4037

Unreachable

Component: Linux
Version: 3.10.108
Description: A vulnerability was found in the fs/inode.c:inode_init_owner() function logic of the LInux kernel that allows local users to create files for the XFS file-system with an unintended group ownership and...
Severity: High
Risk Score: 7.8
EPSS Percentile: 3.3%

CVE-2021-3847

Component: Linux
Version: 3.10.108
Description: An unauthorized access to the execution of the setuid file with capabilities flaw in the Linux kernel OverlayFS subsystem was found in the way user copying a capable file from a nosuid mount into anot...
Severity: High
Risk Score: 7.8
EPSS Percentile: 0.9%

CVE-2021-38166

Unreachable

Component: Linux
Version: 3.10.108
Description: In kernel/bpf/hashtab.c in the Linux kernel through 5.13.8, there is an integer overflow and out-of-bounds write when many elements are placed in a single bucket. NOTE: exploitation might be impractic...
Severity: High
Risk Score: 7.8
EPSS Percentile: 24.4%

CVE-2021-37576 🔥 PoC

Component: Linux
Version: 3.10.108
Description: arch/powerpc/kvm/book3s_rtas.c in the Linux kernel through 5.13.5 on the powerpc platform allows KVM guest OS users to cause host OS memory corruption via rtas_args.nargs, aka CID-f62f3c20647e.
Severity: High
Risk Score: 7.8
EPSS Percentile: 35.1%

CVE-2021-3612

Component: Linux
Version: 3.10.108
Description: An out-of-bounds memory write flaw was found in the Linux kernel's joystick devices subsystem in versions before 5.9-rc1, in the way the user calls ioctl JSIOCSBTNMAP. This flaw allows a local user to...
Severity: High
Risk Score: 7.8
EPSS Percentile: 18.8%

CVE-2021-3483

Component: Linux
Version: 3.10.108
Description: A flaw was found in the Nosy driver in the Linux kernel. This issue allows a device to be inserted twice into a doubly-linked list, leading to a use-after-free when one of these devices is removed. Th...
Severity: High
Risk Score: 7.8
EPSS Percentile: 33.9%

CVE-2021-3444

Component: Linux
Version: 3.10.108
Description: The bpf verifier in the Linux kernel did not properly handle mod32 destination register truncation when the source register was known to be 0. A local attacker with the ability to load bpf programs co...
Severity: High
Risk Score: 7.8
EPSS Percentile: 17.2%

CVE-2021-3347 🔥 PoC

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 5.10.11. PI futexes have a kernel stack use-after-free during fault handling, allowing local users to execute code in the kernel, aka CID-34b1a1ce14...
Severity: High
Risk Score: 7.8
EPSS Percentile: 50.2%

CVE-2021-33034 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 5.12.4, net/bluetooth/hci_event.c has a use-after-free when destroying an hci_chan, aka CID-5c4c8c954409. This leads to writing an arbitrary value.
Severity: High
Risk Score: 7.8
EPSS Percentile: 37.4%

CVE-2021-33033 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The Linux kernel before 5.11.14 has a use-after-free in cipso_v4_genopt in net/ipv4/cipso_ipv4.c because the CIPSO and CALIPSO refcounting for the DOI definitions is mishandled, aka CID-ad5d07f4a9cd. ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 38.4%

CVE-2021-29154

Component: Linux
Version: 3.10.108
Description: BPF JIT compilers in the Linux kernel through 5.11.12 have incorrect computation of branch displacements, allowing them to execute arbitrary code within the kernel context. This affects arch/x86/net/b...
Severity: High
Risk Score: 7.8
EPSS Percentile: 11.3%

CVE-2021-28952

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 5.11.8. The sound/soc/qcom/sdm845.c soundwire device driver has a buffer overflow when an unexpected port ID number is encountered, aka CID-1c668e1c...
Severity: High
Risk Score: 7.8
EPSS Percentile: 44.5%

CVE-2021-27365 🔥 PoC

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 5.11.3. Certain iSCSI data structures do not have appropriate length constraints or checks, and can exceed the PAGE_SIZE value. An unprivileged user...
Severity: High
Risk Score: 7.8
EPSS Percentile: 57.3%

CVE-2021-22555 🔥 Commercial Exploit

Reachable

Component: Linux
Version: 3.10.108
Description: A heap out-of-bounds write affecting Linux since v2.6.19-rc1 was discovered in net/netfilter/x_tables.c. This allows an attacker to gain privileges or cause a DoS (via heap memory corruption) through ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 99.3%

CVE-2021-20268

Component: Linux
Version: 3.10.108
Description: An out-of-bounds access flaw was found in the Linux kernel's implementation of the eBPF code verifier in the way a user running the eBPF script calls dev_map_init_map or sock_map_alloc. This flaw allo...
Severity: High
Risk Score: 7.8
EPSS Percentile: 48.2%

CVE-2020-36385

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.10. drivers/infiniband/core/ucma.c has a use-after-free because the ctx is reached via the ctx_list in some ucma_migrate_id situations where ucma_c...
Severity: High
Risk Score: 7.8
EPSS Percentile: 17.4%

CVE-2020-36313

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.7. The KVM subsystem allows out-of-range access to memslots after a deletion, aka CID-0774a964ef56. This affects arch/s390/kvm/kvm-s390.c, include/...
Severity: High
Risk Score: 7.8
EPSS Percentile: 18.6%

CVE-2020-35519

Unreachable

Component: Linux
Version: 3.10.108
Description: An out-of-bounds (OOB) memory access flaw was found in x25_bind in net/x25/af_x25.c in the Linux kernel version v5.12-rc5. A bounds check failure allows a local attacker with a user account on the sys...
Severity: High
Risk Score: 7.8

EPSS Percentile: 31.0%

CVE-2020-29661 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: A locking issue was discovered in the tty subsystem of the Linux kernel through 5.9.13. drivers/tty/tty_jobctrl.c allows a use-after-free attack against TIOCSPGRP, aka CID-54ffccbf053b.
Severity: High
Risk Score: 7.8
EPSS Percentile: 71.8%

CVE-2020-27786 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A flaw was found in the Linux kernel's implementation of MIDI, where an attacker with a local account and the permissions to issue ioctl commands to midi devices could trigger a use-after-free issue. ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 90.7%

CVE-2020-25671 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A vulnerability was found in Linux Kernel, where a refcount leak in llcp_sock_connect() causing use-after-free which might lead to privilege escalations.
Severity: High
Risk Score: 7.8
EPSS Percentile: 33.6%

CVE-2020-25670 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A vulnerability was found in Linux Kernel where refcount leak in llcp_sock_bind() causing use-after-free which might lead to privilege escalations.
Severity: High
Risk Score: 7.8
EPSS Percentile: 26.4%

CVE-2020-25669 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A vulnerability was found in the Linux Kernel where the function sunkbd_reinit having been scheduled by sunkbd_interrupt before sunkbd being freed. Though the dangling pointer is set to NULL in sunkbd...
Severity: High

Risk Score: 7.8
EPSS Percentile: 27.2%

CVE-2020-14381

Component: Linux
Version: 3.10.108
Description: A flaw was found in the Linux kernel's futex implementation. This flaw allows a local attacker to corrupt system memory or escalate their privileges when creating a futex on a filesystem that is about...
Severity: High
Risk Score: 7.8
EPSS Percentile: 68.3%

CVE-2020-14351

Component: Linux
Version: 3.10.108
Description: A flaw was found in the Linux kernel. A use-after-free memory flaw was found in the perf subsystem allowing a local attacker with permission to monitor perf events to corrupt memory and possibly escal...
Severity: High
Risk Score: 7.8
EPSS Percentile: 4.4%

CVE-2020-13974 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel 4.4 through 5.7.1. drivers/tty/vt/keyboard.c has an integer overflow if k_ascii is called several times in a row, aka CID-b86dab054059. NOTE: Members in the...
Severity: High
Risk Score: 7.8
EPSS Percentile: 36.0%

CVE-2020-12657

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.6.5. There is a use-after-free in block/bfq-iosched.c related to bfq_idle_slice_timer_body.
Severity: High
Risk Score: 7.8
EPSS Percentile: 28.1%

CVE-2020-12653

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was found in Linux kernel before 5.5.4. The mwifiex_cmd_append_vsie_tlv() function in drivers/net/wireless/marvell/mwifiex/scan.c allows local users to gain privileges or cause a denial of se...
Severity: High
Risk Score: 7.8
EPSS Percentile: 42.2%

CVE-2019-7221 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The KVM implementation in the Linux kernel through 4.20.5 has a Use-after-Free.
Severity: High
Risk Score: 7.8
EPSS Percentile: 48.4%

CVE-2019-25045 🔥 PoC

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.0.19. The XFRM subsystem has a use-after-free, related to an xfrm_state_fini panic, aka CID-dbb2483b2a46.
Severity: High
Risk Score: 7.8
EPSS Percentile: 37.4%

CVE-2019-19816 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel 5.0.21, mounting a crafted btrfs filesystem image and performing some operations can cause slab-out-of-bounds write access in __btrfs_map_block in fs/btrfs/volumes.c, because a val...
Severity: High
Risk Score: 7.8
EPSS Percentile: 59.1%

CVE-2019-19543

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 5.1.6, there is a use-after-free in serial_ir_init_module() in drivers/media/rc/serial_ir.c.
Severity: High
Risk Score: 7.8
EPSS Percentile: 28.9%

CVE-2019-19448 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel 5.0.21 and 5.3.11, mounting a crafted btrfs filesystem image, performing some operations, and then making a syncfs system call can lead to a use-after-free in try_merge_free_space ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 69.4%

CVE-2019-19447 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel 5.0.21, mounting a crafted ext4 filesystem image, performing some operations, and unmounting can lead to a use-after-free in ext4_put_super in fs/ext4/super.c, related to dump_orph...
Severity: High
Risk Score: 7.8
EPSS Percentile: 81.4%

CVE-2019-19377 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel 5.0.21, mounting a crafted btrfs filesystem image, performing some operations, and unmounting can lead to a use-after-free in btrfs_queue_work in fs/btrfs/async-thread.c.
Severity: High
Risk Score: 7.8
EPSS Percentile: 65.7%

CVE-2019-19252

Unreachable

Component: Linux
Version: 3.10.108
Description: vcs_write in drivers/tty/vt/vc_screen.c in the Linux kernel through 5.3.13 does not prevent write access to vcsu devices, aka CID-0c9acb1af77a.
Severity: High
Risk Score: 7.8
EPSS Percentile: 35.6%

CVE-2019-19241 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 5.4.2, the io_uring feature leads to requests that inadvertently have UID

0 and full capabilities, aka CID-181e448d8709. This is related to fs/io-wq.c, fs/io_uring.c, and ne...
Severity: High
Risk Score: 7.8
EPSS Percentile: 75.2%

CVE-2019-18675 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The Linux kernel through 5.3.13 has a start_offset+size Integer Overflow in cpia2_remap_buffer in drivers/media/usb/cpia2/cpia2_core.c because cpia2 has its own mmap implementation. This allows local ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 33.5%

CVE-2019-15927

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 4.20.2. An out-of-bounds access exists in the function build_audio_procunit in the file sound/usb/mixer.c.
Severity: High
Risk Score: 7.8
EPSS Percentile: 22.9%

CVE-2019-15117

Unreachable

Component: Linux
Version: 3.10.108
Description: parse_audio_mixer_unit in sound/usb/mixer.c in the Linux kernel through 5.2.9 mishandles a short descriptor, leading to out-of-bounds memory access.
Severity: High
Risk Score: 7.8
EPSS Percentile: 27.7%

CVE-2019-14835 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A buffer overflow flaw was found, in versions from 2.6.34 to 5.2.x, in the way Linux kernel's vhost functionality that translates virtqueue buffers to IOVs, logged the buffer descriptors during migrat...
Severity: High
Risk Score: 7.8
EPSS Percentile: 75.3%

CVE-2019-14816 🔥 PoC

Component: Linux
Version: 3.10.108

Description: There is heap-based buffer overflow in kernel, all versions up to, excluding 5.3, in the marvell wifi chip driver in Linux kernel, that allows local users to cause a denial of service(system crash) or...
Severity: High
Risk Score: 7.8
EPSS Percentile: 52.0%

CVE-2019-14814 🔥 PoC

Component: Linux
Version: 3.10.108
Description: There is heap-based buffer overflow in Linux kernel, all versions up to, excluding 5.3, in the marvell wifi chip driver in Linux kernel, that allows local users to cause a denial of service(system cra...
Severity: High
Risk Score: 7.8
EPSS Percentile: 48.6%

CVE-2019-12454

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in wcd9335_codec_enable_dec in sound/soc/codecs/wcd9335.c in the Linux kernel through 5.1.5. It uses kstrndup instead of kmemdup_nul, which allows attackers to have an unspecif...
Severity: High
Risk Score: 7.8
EPSS Percentile: 32.3%

CVE-2019-11487 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The Linux kernel before 5.1-rc5 allows page->_refcount reference count overflow, with resultant use-after-free issues, if about 140 GiB of RAM exists. This is related to fs/fuse/dev.c, fs/pipe.c, fs/s...
Severity: High
Risk Score: 7.8
EPSS Percentile: 59.0%

CVE-2018-8822

Component: Linux
Version: 3.10.108
Description: Incorrect buffer length handling in the ncp_read_kernel function in fs/ncpfs/ncplib_kernel.c in the Linux kernel through 4.15.11, and in drivers/staging/ncpfs/ncplib_kernel.c in the Linux kernel 4.16-...
Severity: High
Risk Score: 7.8
EPSS Percentile: 18.6%

CVE-2018-8781

Component: Linux
Version: 3.10.108
Description: The udl_fb_mmap function in drivers/gpu/drm/udl/udl_fb.c at the Linux kernel version 3.4 and up to and including 4.15 has an integer-overflow vulnerability allowing local users with access to the udld...
Severity: High
Risk Score: 7.8
EPSS Percentile: 28.8%

CVE-2018-6927

Component: Linux
Version: 3.10.108
Description: The futex_requeue function in kernel/futex.c in the Linux kernel before 4.14.15 might allow attackers to cause a denial of service (integer overflow) or possibly have unspecified other impact by trigg...
Severity: High
Risk Score: 7.8
EPSS Percentile: 24.5%

CVE-2018-6555

Component: Linux
Version: 3.10.108
Description: The irda_setsockopt function in net/irda/af_irda.c and later in drivers/staging/irda/net/af_irda.c in the Linux kernel before 4.17 allows local users to cause a denial of service (ias_object use-after...
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.6%

CVE-2018-5344

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel through 4.14.13, drivers/block/loop.c mishandles lo_release serialization, which allows attackers to cause a denial of service (__lock_acquire use-after-free) or possibly have unsp...
Severity: High
Risk Score: 7.8
EPSS Percentile: 12.8%

CVE-2018-5332

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel through 3.2, the rds_message_alloc_sgs() function does not validate a value that is used during DMA page allocation, leading to a heap-based out-of-bounds write (related to the rds...
Severity: High
Risk Score: 7.8
EPSS Percentile: 24.3%

CVE-2018-25020

Unreachable

Component: Linux
Version: 3.10.108
Description: The BPF subsystem in the Linux kernel before 4.17 mishandles situations with a long jump over an instruction sequence where inner instructions require substantial expansions into multiple BPF instruct...
Severity: High
Risk Score: 7.8
EPSS Percentile: 4.8%

CVE-2018-25015 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 4.14.16. There is a use-after-free in net/sctp/socket.c for a held lock after a peel off, aka CID-a0ff660058b8.
Severity: High
Risk Score: 7.8
EPSS Percentile: 37.4%

CVE-2018-20976

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in fs/xfs/xfs_super.c in the Linux kernel before 4.18. A use after free exists, related to xfs_fs_fill_super failure.
Severity: High
Risk Score: 7.8
EPSS Percentile: 25.7%

CVE-2018-20856

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 4.18.7. In block/blk-core.c, there is an __blk_drain_queue() use-after-free because a certain error case is mishandled.
Severity: High
Risk Score: 7.8
EPSS Percentile: 6.9%

CVE-2018-20854

Unreachable

Component: Linux
Version: 3.10.108

Description: An issue was discovered in the Linux kernel before 4.20. drivers/phy/mscc/phy-ocelot-serdes.c has an off-by-one error with a resultant ctrl->phys out-of-bounds read.
Severity: High
Risk Score: 7.8
EPSS Percentile: 23.2%

CVE-2018-19824

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel through 4.19.6, a local user could exploit a use-after-free in the ALSA driver by supplying a malicious USB Sound device (with zero interfaces) that is mishandled in usb_audio_prob...
Severity: High
Risk Score: 7.8
EPSS Percentile: 22.3%

CVE-2018-18281 🔥 PoC

Component: Linux
Version: 3.10.108
Description: Since Linux kernel version 3.2, the mremap() syscall performs TLB flushes after dropping pagetable locks. If a syscall such as ftruncate() removes entries from the pagetables of a task that is in the ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 61.7%

CVE-2018-16276

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in yurex_read in drivers/usb/misc/yurex.c in the Linux kernel before 4.17.7. Local attackers could use user access read/writes with incorrect bounds checking in the yurex USB d...
Severity: High
Risk Score: 7.8
EPSS Percentile: 24.6%

CVE-2018-14734

Component: Linux
Version: 3.10.108
Description: drivers/infiniband/core/ucma.c in the Linux kernel through 4.17.11 allows ucma_leave_multicast to access a certain data structure after a cleanup step in ucma_process_join, which allows attackers to c...
Severity: High
Risk Score: 7.8
EPSS Percentile: 17.1%

CVE-2018-13406

Unreachable

Component: Linux
Version: 3.10.108
Description: An integer overflow in the uvesafb_setcmap function in drivers/video/fbdev/uvesafb.c in the Linux kernel before 4.17.4 could result in local attackers being able to crash the kernel or potentially ele...
Severity: High
Risk Score: 7.8
EPSS Percentile: 4.5%

CVE-2018-13405 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The inode_init_owner function in fs/inode.c in the Linux kernel through 3.16 allows local users to create files with an unintended group ownership, in a scenario where a directory is SGID to a certain...
Severity: High
Risk Score: 7.8
EPSS Percentile: 38.4%

CVE-2018-12233

Unreachable

Component: Linux
Version: 3.10.108
Description: In the ea_get function in fs/jfs/xattr.c in the Linux kernel through 4.17.1, a memory corruption bug in JFS can be triggered by calling setxattr twice with two different extended attribute names on th...
Severity: High
Risk Score: 7.8
EPSS Percentile: 23.3%

CVE-2018-10879 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause a use-after-free in ext4_xattr_set_entry function and a denial of service or unspecified other impact may occur by renami...
Severity: High
Risk Score: 7.8
EPSS Percentile: 12.2%

CVE-2018-10878 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bounds write and a denial of service or unspecified other impact is possible by mounting and operating a crafte...
Severity: High
Risk Score: 7.8
EPSS Percentile: 18.5%

CVE-2018-10853

Component: Linux
Version: 3.10.108
Description: A flaw was found in the way Linux kernel KVM hypervisor before 4.18 emulated instructions such as sgdt/sidt/fxsave/fxrstor. It did not check current privilege(CPL) level while emulating unprivileged i...
Severity: High
Risk Score: 7.8
EPSS Percentile: 14.8%

CVE-2018-10675

Unreachable

Component: Linux
Version: 3.10.108
Description: The do_get_mempolicy function in mm/mempolicy.c in the Linux kernel before 4.12.9 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted...
Severity: High
Risk Score: 7.8
EPSS Percentile: 17.4%

CVE-2017-9986

Component: Linux
Version: 3.10.108
Description: The intr function in sound/oss/msnd_pinnacle.c in the Linux kernel through 4.11.7 allows local users to cause a denial of service (over-boundary access) or possibly have unspecified other impact by ch...
Severity: High
Risk Score: 7.8
EPSS Percentile: 27.8%

CVE-2017-9985

Component: Linux
Version: 3.10.108
Description: The snd_msndmidi_input_read function in sound/isa/msnd/msnd_midi.c in the Linux kernel through 4.11.7 allows local users to cause a denial of service (over-boundary access) or possibly have unspecifie...
Severity: High
Risk Score: 7.8
EPSS Percentile: 31.0%

CVE-2017-9984

Unreachable

Component: Linux
Version: 3.10.108
Description: The snd_msnd_interrupt function in sound/isa/msnd/msnd_pinnacle.c in the Linux kernel through 4.11.7 allows local users to cause a denial of service (over-boundary access) or possibly have unspecified...
Severity: High

Risk Score: 7.8
EPSS Percentile: 29.7%

CVE-2017-9077

Reachable

Component: Linux
Version: 3.10.108
Description: The tcp_v6_syn_recv_sock function in net/ipv6/tcp_ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified o...
Severity: High
Risk Score: 7.8
EPSS Percentile: 73.0%

CVE-2017-9076

Component: Linux
Version: 3.10.108
Description: The dccp_v6_request_recv_sock function in net/dccp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 26.3%

CVE-2017-9075

Component: Linux
Version: 3.10.108
Description: The sctp_v6_create_accept_sk function in net/sctp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified o...
Severity: High
Risk Score: 7.8
EPSS Percentile: 24.4%

CVE-2017-9074

Component: Linux
Version: 3.10.108
Description: The IPv6 fragmentation implementation in the Linux kernel through 4.11.1 does not consider that the nexthdr field may be associated with an invalid option, which allows local users to cause a denial o...
Severity: High
Risk Score: 7.8
EPSS Percentile: 24.4%

CVE-2017-8824 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The dccp_disconnect function in net/dccp/proto.c in the Linux kernel through 4.14.3 allows local users to gain privileges or cause a denial of service (use-after-free) via an AF_UNSPEC connect system ...
Severity: High

Risk Score: 7.8
EPSS Percentile: 72.5%

CVE-2017-7518

Component: Linux
Version: 3.10.108
Description: A flaw was found in the Linux kernel before version 4.12 in the way the KVM module processed the trap flag(TF) bit in EFLAGS during emulation of the syscall instruction, which leads to a debug excepti...
Severity: High
Risk Score: 7.8
EPSS Percentile: 26.8%

CVE-2017-7487

Component: Linux
Version: 3.10.108
Description: The ipxitf_ioctl function in net/ipx/af_ipx.c in the Linux kernel through 4.11.1 mishandles reference counts, which allows local users to cause a denial of service (use-after-free) or possibly have un...
Severity: High
Risk Score: 7.8
EPSS Percentile: 24.4%

CVE-2017-7187

Unreachable

Component: Linux
Version: 3.10.108
Description: The sg_ioctl function in drivers/scsi/sg.c in the Linux kernel through 4.10.4 allows local users to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact vi...
Severity: High
Risk Score: 7.8
EPSS Percentile: 25.0%

CVE-2017-6345

Component: Linux
Version: 3.10.108
Description: The LLC subsystem in the Linux kernel before 4.9.13 does not ensure that a certain destructor exists in required circumstances, which allows local users to cause a denial of service (BUG_ON) or possib...
Severity: High
Risk Score: 7.8
EPSS Percentile: 23.8%

CVE-2017-5669

Unreachable

Component: Linux
Version: 3.10.108
Description: The do_shmat function in ipc/shm.c in the Linux kernel through 4.9.12 does not restrict the address

calculated by a certain rounding operation, which allows local users to map page zero, and consequen...
Severity: High
Risk Score: 7.8
EPSS Percentile: 18.8%

CVE-2017-2647

Component: Linux
Version: 3.10.108
Description: The KEYS subsystem in the Linux kernel before 3.18 allows local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) via vectors involving a NULL value for...
Severity: High
Risk Score: 7.8
EPSS Percentile: 11.9%

CVE-2017-18595

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 4.14.11. A double free may be caused by the function allocate_trace_buffer in the file kernel/trace/trace.c.
Severity: High
Risk Score: 7.8
EPSS Percentile: 13.2%

CVE-2017-18552

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in net/rds/af_rds.c in the Linux kernel before 4.11. There is an out of bounds write and read in the function rds_recv_track_latency.
Severity: High
Risk Score: 7.8
EPSS Percentile: 33.2%

CVE-2017-18509 🔥 PoC

Reachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in net/ipv6/ip6mr.c in the Linux kernel before 4.11. By setting a specific socket option, an attacker can control a pointer in kernel land and cause an inet_csk_listen_stop gen...
Severity: High
Risk Score: 7.8
EPSS Percentile: 54.8%

CVE-2017-18255

Unreachable

Component: Linux
Version: 3.10.108
Description: The perf_cpu_time_max_percent_handler function in kernel/events/core.c in the Linux kernel before 4.11 allows local users to cause a denial of service (integer overflow) or possibly have unspecified o...
Severity: High
Risk Score: 7.8
EPSS Percentile: 30.4%

CVE-2017-18222

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 4.12, Hisilicon Network Subsystem (HNS) does not consider the ETH_SS_PRIV_FLAGS case when retrieving sset_count data, which allows local users to cause a denial of service (...
Severity: High
Risk Score: 7.8
EPSS Percentile: 7.8%

CVE-2017-18079

Unreachable

Component: Linux
Version: 3.10.108
Description: drivers/input/serio/i8042.c in the Linux kernel before 4.12.4 allows attackers to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact becaus...
Severity: High
Risk Score: 7.8
EPSS Percentile: 25.0%

CVE-2017-17806

Reachable

Component: Linux
Version: 3.10.108
Description: The HMAC implementation (crypto/hmac.c) in the Linux kernel before 4.14.8 does not validate that the underlying cryptographic hash algorithm is unkeyed, allowing a local attacker able to use the AF_AL...
Severity: High
Risk Score: 7.8
EPSS Percentile: 12.2%

CVE-2017-17805

Component: Linux
Version: 3.10.108
Description: The Salsa20 encryption algorithm in the Linux kernel before 4.14.8 does not correctly handle zero-length inputs, allowing a local attacker able to use the AF_ALG-based skcipher interface (CONFIG_CRYPT...
Severity: High
Risk Score: 7.8
EPSS Percentile: 30.1%

CVE-2017-17450

Unreachable

Component: Linux
Version: 3.10.108
Description: net/netfilter/xt_osf.c in the Linux kernel through 4.14.4 does not require the CAP_NET_ADMIN capability for add_callback and remove_callback operations, which allows local users to bypass intended acc...
Severity: High
Risk Score: 7.8
EPSS Percentile: 17.0%

CVE-2017-17448

Unreachable

Component: Linux
Version: 3.10.108
Description: net/netfilter/nfnetlink_cthelper.c in the Linux kernel through 4.14.4 does not require the CAP_NET_ADMIN capability for new, get, and del operations, which allows local users to bypass intended access...
Severity: High
Risk Score: 7.8
EPSS Percentile: 20.5%

CVE-2017-16939 🔥 PoC

Reachable

Component: Linux
Version: 3.10.108
Description: The XFRM dump policy implementation in net/xfrm/xfrm_user.c in the Linux kernel before 4.13.11 allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted SO_RCVB...
Severity: High
Risk Score: 7.8
EPSS Percentile: 92.2%

CVE-2017-16526

Component: Linux
Version: 3.10.108
Description: drivers/uwb/uwbd.c in the Linux kernel before 4.13.6 allows local users to cause a denial of service (general protection fault and system crash) or possibly have unspecified other impact via a crafted...
Severity: High
Risk Score: 7.8
EPSS Percentile: 32.3%

CVE-2017-15649 🔥 PoC

Reachable

Component: Linux
Version: 3.10.108

Description: net/packet/af_packet.c in the Linux kernel before 4.13.6 allows local users to gain privileges via crafted system calls that trigger mishandling of packet_fanout data structures, because of a race con...
Severity: High
Risk Score: 7.8
EPSS Percentile: 58.0%

CVE-2017-15115

Unreachable

Component: Linux
Version: 3.10.108
Description: The sctp_do_peeloff function in net/sctp/socket.c in the Linux kernel before 4.14 does not check whether the intended netns is used in a peel-off action, which allows local users to cause a denial of ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 27.4%

CVE-2017-11473

Unreachable

Component: Linux
Version: 3.10.108
Description: Buffer overflow in the mp_override_legacy_irq() function in arch/x86/kernel/acpi/boot.c in the Linux kernel through 3.2 allows local users to gain privileges via a crafted ACPI table.
Severity: High
Risk Score: 7.8
EPSS Percentile: 27.0%

CVE-2017-11176 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The mq_notify function in the Linux kernel through 4.11.9 does not set the sock pointer to NULL upon entry into the retry logic. During a user-space close of a Netlink socket, it allows attackers to c...
Severity: High
Risk Score: 7.8
EPSS Percentile: 95.9%

CVE-2017-10663

Unreachable

Component: Linux
Version: 3.10.108
Description: The sanity_check_ckpt function in fs/f2fs/super.c in the Linux kernel before 4.12.4 does not validate the blkoff and segno arrays, which allows local users to gain privileges via unspecified vectors.
Severity: High
Risk Score: 7.8
EPSS Percentile: 27.2%

CVE-2017-10662

Unreachable

Component: Linux
Version: 3.10.108
Description: The sanity_check_raw_super function in fs/f2fs/super.c in the Linux kernel before 4.11.1 does not validate the segment count, which allows local users to gain privileges via unspecified vectors.
Severity: High
Risk Score: 7.8
EPSS Percentile: 28.5%

CVE-2016-9793 🔥 Commercial Exploit

Unreachable

Component: Linux
Version: 3.10.108
Description: The sock_setsockopt function in net/core/sock.c in the Linux kernel before 4.8.14 mishandles negative values of sk_sndbuf and sk_rcvbuf, which allows local users to cause a denial of service (memory c...
Severity: High
Risk Score: 7.8
EPSS Percentile: 83.6%

CVE-2016-9755

Reachable

Component: Linux
Version: 3.10.108
Description: The netfilter subsystem in the Linux kernel before 4.9 mishandles IPv6 reassembly, which allows local users to cause a denial of service (integer overflow, out-of-bounds write, and GPF) or possibly ha...
Severity: High
Risk Score: 7.8
EPSS Percentile: 15.7%

CVE-2016-9084

Unreachable

Component: Linux
Version: 3.10.108
Description: drivers/vfio/pci/vfio_pci_intrs.c in the Linux kernel through 4.8.11 misuses the kzalloc function, which allows local users to cause a denial of service (integer overflow) or have unspecified other im...
Severity: High
Risk Score: 7.8
EPSS Percentile: 15.7%

CVE-2016-8632

Unreachable

Component: Linux
Version: 3.10.108

Description: The tipc_msg_build function in net/tipc/msg.c in the Linux kernel through 4.8.11 does not validate the relationship between the minimum fragment length and the maximum packet size, which allows local ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 28.9%

CVE-2016-5870

Component: Linux
Version: 3.10.108
Description: The msm_ipc_router_close function in net/ipc_router/ipc_router_socket.c in the ipc_router component for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM...
Severity: High
Risk Score: 7.8
EPSS Percentile: 22.5%

CVE-2016-5342

Component: Linux
Version: 3.10.108
Description: Heap-based buffer overflow in the wcnss_wlan_write function in drivers/net/wireless/wcnss/wcnss_wlan.c in the wcnss_wlan device driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (...
Severity: High
Risk Score: 7.8
EPSS Percentile: 69.0%

CVE-2016-5340

Component: Linux
Version: 3.10.108
Description: The is_ashmem_file function in drivers/staging/android/ashmem.c in a certain Qualcomm Innovation Center (QuIC) Android patch for the Linux kernel 3.x mishandles pointer validation within the KGSL Linu...
Severity: High
Risk Score: 7.8
EPSS Percentile: 4.3%

CVE-2016-3672 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The arch_pick_mmap_layout function in arch/x86/mm/mmap.c in the Linux kernel through 4.5.2 does not properly randomize the legacy base address, which makes it easier for local users to defeat the inte...
Severity: High
Risk Score: 7.8
EPSS Percentile: 2.2%

CVE-2016-3070

Unreachable

Component: Linux
Version: 3.10.108
Description: The trace_writeback_dirty_page implementation in include/trace/events/writeback.h in the Linux kernel before 4.4 improperly interacts with mm/migrate.c, which allows local users to cause a denial of s...
Severity: High
Risk Score: 7.8
EPSS Percentile: 24.9%

CVE-2016-2854 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The aufs module for the Linux kernel 3.x and 4.x does not properly maintain POSIX ACL xattr data, which allows local users to gain privileges by leveraging a group-writable setgid directory.
Severity: High
Risk Score: 7.8
EPSS Percentile: 38.9%

CVE-2016-2853 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The aufs module for the Linux kernel 3.x and 4.x does not properly restrict the mount namespace, which allows local users to gain privileges by mounting an aufs filesystem on top of a FUSE filesystem,...
Severity: High
Risk Score: 7.8
EPSS Percentile: 44.7%

CVE-2016-2143

Component: Linux
Version: 3.10.108
Description: The fork implementation in the Linux kernel before 4.5 on s390 platforms mishandles the case of four page-table levels, which allows local users to cause a denial of service (system crash) or possibly...
Severity: High
Risk Score: 7.8
EPSS Percentile: 41.6%

CVE-2016-2068

Component: Linux
Version: 3.10.108
Description: The MSM QDSP6 audio driver (aka sound driver) for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to gain ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 37.9%

CVE-2016-2067

Component: Linux
Version: 3.10.108
Description: drivers/gpu/msm/kgsl.c in the MSM graphics driver (aka GPU driver) for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, mish...
Severity: High
Risk Score: 7.8
EPSS Percentile: 32.7%

CVE-2016-2066

Component: Linux
Version: 3.10.108
Description: Integer signedness error in the MSM QDSP6 audio driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers...
Severity: High
Risk Score: 7.8
EPSS Percentile: 50.9%

CVE-2016-2065

Component: Linux
Version: 3.10.108
Description: sound/soc/msm/qdsp6v2/msm-audio-effects-q6-v2.c in the MSM QDSP6 audio driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other pro...
Severity: High
Risk Score: 7.8
EPSS Percentile: 51.5%

CVE-2016-2064

Component: Linux
Version: 3.10.108
Description: sound/soc/msm/qdsp6v2/msm-audio-effects-q6-v2.c in the MSM QDSP6 audio driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other pro...
Severity: High
Risk Score: 7.8
EPSS Percentile: 47.4%

CVE-2016-2063

Component: Linux
Version: 3.10.108
Description: Stack-based buffer overflow in the supply_lm_input_write function in drivers/thermal/supply_lm_core.c in the MSM Thermal driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) A...
Severity: High
Risk Score: 7.8
EPSS Percentile: 33.3%

CVE-2016-2062

Component: Linux
Version: 3.10.108
Description: The adreno_perfcounter_query_group function in drivers/gpu/msm/adreno_perfcounter.c in the Adreno GPU driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contribution...
Severity: High
Risk Score: 7.8
EPSS Percentile: 18.1%

CVE-2016-2061

Component: Linux
Version: 3.10.108
Description: Integer signedness error in the MSM V4L2 video driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 52.9%

CVE-2016-1583 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The ecryptfs_privileged_open function in fs/ecryptfs/kthread.c in the Linux kernel before 4.6.3 allows local users to gain privileges or cause a denial of service (stack memory consumption) via vector...
Severity: High
Risk Score: 7.8
EPSS Percentile: 51.9%

CVE-2016-1576 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The overlayfs implementation in the Linux kernel through 4.5.2 does not properly restrict the mount namespace, which allows local users to gain privileges by mounting an overlayfs filesystem on top of...
Severity: High
Risk Score: 7.8
EPSS Percentile: 57.0%

CVE-2016-1575 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The overlayfs implementation in the Linux kernel through 4.5.2 does not properly maintain POSIX ACL xattr data, which allows local users to gain privileges by leveraging a group-writable setgid direct...
Severity: High
Risk Score: 7.8
EPSS Percentile: 66.3%

CVE-2016-10907

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in drivers/iio/dac/ad5755.c in the Linux kernel before 4.8.6. There is an out of bounds write in the function ad5755_parse_dt.
Severity: High
Risk Score: 7.8
EPSS Percentile: 26.5%

CVE-2016-10905

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in fs/gfs2/rgrp.c in the Linux kernel before 4.8. A use-after-free is caused by the functions gfs2_clear_rgrpd and read_rindex_entry.
Severity: High
Risk Score: 7.8
EPSS Percentile: 21.9%

CVE-2016-10044

Unreachable

Component: Linux
Version: 3.10.108
Description: The aio_mount function in fs/aio.c in the Linux kernel before 4.7.7 does not properly restrict execute access, which makes it easier for local users to bypass intended SELinux W^X policy restrictions,...
Severity: High
Risk Score: 7.8
EPSS Percentile: 2.1%

CVE-2016-0758

Unreachable

Component: Linux
Version: 3.10.108
Description: Integer overflow in lib/asn1_decoder.c in the Linux kernel before 4.6 allows local users to gain privileges via crafted ASN.1 data.
Severity: High
Risk Score: 7.8
EPSS Percentile: 32.2%

CVE-2015-8967

Component: Linux
Version: 3.10.108
Description: arch/arm64/kernel/sys.c in the Linux kernel before 4.0 allows local users to bypass the "strict page permissions" protection mechanism and modify the system-call table, and consequently gain privilege...

Severity: High
Risk Score: 7.8
EPSS Percentile: 22.8%

CVE-2015-8966

Unreachable

Component: Linux
Version: 3.10.108
Description: arch/arm/kernel/sys_oabi-compat.c in the Linux kernel before 4.4 allows local users to gain privileges via a crafted (1) F_OFD_GETLK, (2) F_OFD_SETLK, or (3) F_OFD_SETLKW command in an fcntl64 system ...
Severity: High
Risk Score: 7.8
EPSS Percentile: 40.6%

CVE-2015-8961

Unreachable

Component: Linux
Version: 3.10.108
Description: The __ext4_journal_stop function in fs/ext4/ext4_jbd2.c in the Linux kernel before 4.3.3 allows local users to gain privileges or cause a denial of service (use-after-free) by leveraging improper acce...
Severity: High
Risk Score: 7.8
EPSS Percentile: 47.9%

CVE-2015-8539

Unreachable

Component: Linux
Version: 3.10.108
Description: The KEYS subsystem in the Linux kernel before 4.4 allows local users to gain privileges or cause a denial of service (BUG) via crafted keyctl commands that negatively instantiate a key, related to sec...
Severity: High
Risk Score: 7.8
EPSS Percentile: 26.0%

CVE-2015-1328 🔥 Commercial Exploit

Component: Linux
Version: 3.10.108
Description: The overlayfs implementation in the linux (aka Linux kernel) package before 3.19.0-21.21 in Ubuntu through 15.04 does not properly check permissions for file creation in the upper filesystem directory...
Severity: High
Risk Score: 7.8
EPSS Percentile: 99.5%

CVE-2015-0571

Component: Linux
Version: 3.10.108
Description: The WLAN (aka Wi-Fi) driver for the Linux kernel 3.x and 4.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, does not verify authorization for p...
Severity: High
Risk Score: 7.8
EPSS Percentile: 28.6%

CVE-2015-0570

Component: Linux
Version: 3.10.108
Description: Stack-based buffer overflow in the SET_WPS_IE IOCTL implementation in wlan_hdd_hostapd.c in the WLAN (aka Wi-Fi) driver for the Linux kernel 3.x and 4.x, as used in Qualcomm Innovation Center (QuIC) A...
Severity: High
Risk Score: 7.8
EPSS Percentile: 19.4%

CVE-2015-0569 🔥 PoC

Component: Linux
Version: 3.10.108
Description: Heap-based buffer overflow in the private wireless extensions IOCTL implementation in wlan_hdd_wext.c in the WLAN (aka Wi-Fi) driver for the Linux kernel 3.x and 4.x, as used in Qualcomm Innovation Ce...
Severity: High
Risk Score: 7.8
EPSS Percentile: 71.3%

CVE-2015-0568

Component: Linux
Version: 3.10.108
Description: Use-after-free vulnerability in the msm_set_crop function in drivers/media/video/msm/msm_camera.c in the MSM-Camera driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Androi...
Severity: High
Risk Score: 7.8
EPSS Percentile: 63.4%

CVE-2014-9922

Unreachable

Component: Linux
Version: 3.10.108
Description: The eCryptfs subsystem in the Linux kernel before 3.18 allows local users to gain privileges via a large filesystem stack that includes an overlayfs layer, related to fs/ecryptfs/main.c and fs/overlay...
Severity: High
Risk Score: 7.8
EPSS Percentile: 23.0%

CVE-2014-9904

Unreachable

Component: Linux
Version: 3.10.108
Description: The snd_compress_check_input function in sound/core/compress_offload.c in the ALSA subsystem in the Linux kernel before 3.17 does not properly check for an integer overflow, which allows local users t...
Severity: High
Risk Score: 7.8
EPSS Percentile: 22.8%

CVE-2014-9803

Component: Linux
Version: 3.10.108
Description: arch/arm64/include/asm/pgtable.h in the Linux kernel before 3.15-rc5-next-20140519, as used in Android before 2016-07-05 on Nexus 5X and 6P devices, mishandles execute-only pages, which allows attacke...
Severity: High
Risk Score: 7.8
EPSS Percentile: 35.3%

CVE-2014-8369 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The kvm_iommu_map_pages function in virt/kvm/iommu.c in the Linux kernel through 3.17.2 miscalculates the number of pages during the handling of a mapping failure, which allows guest OS users to cause...
Severity: High
Risk Score: 7.8
EPSS Percentile: 43.6%

CVE-2013-7445

Component: Linux
Version: 3.10.108
Description: The Direct Rendering Manager (DRM) subsystem in the Linux kernel through 4.x mishandles requests for Graphics Execution Manager (GEM) objects, which allows context-dependent attackers to cause a denia...
Severity: High
Risk Score: 7.8
EPSS Percentile: 73.6%

CVE-2024-36016

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: tty: n_gsm: fix possible out-of-bounds in gsm0_receive() Assuming the following: - side A configures the n_gsm in basic option mod...
Severity: High

Risk Score: 7.7
EPSS Percentile: 2.2%

CVE-2021-47356

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: mISDN: fix possible use-after-free in HFC_cleanup() This module's remove path calls del_timer(). However, that function does not w...
Severity: High
Risk Score: 7.7
EPSS Percentile: 0.9%

CVE-2019-3900

Component: Linux
Version: 3.10.108
Description: An infinite loop issue was found in the vhost_net kernel module in Linux Kernel up to and including v5.1-rc6, while handling incoming packets in handle_rx(). It could occur if one end sends packets fa...
Severity: High
Risk Score: 7.7
EPSS Percentile: 31.6%

CVE-2018-1000026

Component: Linux
Version: 3.10.108
Description: Linux Linux kernel version at least v4.8 onwards, probably well before contains a Insufficient input validation vulnerability in bnx2x network card driver that can result in DoS: Network card firmware...
Severity: High
Risk Score: 7.7
EPSS Percentile: 74.2%

CVE-2024-49997

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net: ethernet: lantiq_etop: fix memory disclosure When applying padding, the buffer is not zeroed, which results in memory disclos...
Severity: High
Risk Score: 7.5
EPSS Percentile: 56.4%

CVE-2024-42225

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: replace skb_put with skb_put_zero Avoid potentially reusing uninitialized data
Severity: High
Risk Score: 7.5
EPSS Percentile: 35.2%

CVE-2024-27405

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: usb: gadget: ncm: Avoid dropping datagrams of properly parsed NTBs It is observed sometimes when tethering is used over NCM with W...
Severity: High
Risk Score: 7.5
EPSS Percentile: 36.1%

CVE-2023-6200

Component: Linux
Version: 3.10.108
Description: A race condition was found in the Linux Kernel. Under certain conditions, an unauthenticated attacker from an adjacent network could send an ICMPv6 router advertisement packet, causing arbitrary code ...
Severity: High
Risk Score: 7.5
EPSS Percentile: 70.6%

CVE-2023-52340

Reachable

Component: Linux
Version: 3.10.108
Description: The IPv6 implementation in the Linux kernel before 6.3 has a net/ipv6/route.c max_size threshold that can be consumed easily, e.g., leading to a denial of service (network is unreachable errors) when ...
Severity: High
Risk Score: 7.5
EPSS Percentile: 14.9%

CVE-2023-45871

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in drivers/net/ethernet/intel/igb/igb_main.c in the IGB driver in the Linux kernel before 6.5.3. A buffer size may not be adequate for frames larger than the MTU.
Severity: High
Risk Score: 7.5
EPSS Percentile: 4.4%

CVE-2023-39197

Component: Linux
Version: 3.10.108
Description: An out-of-bounds read vulnerability was found in Netfilter Connection Tracking (conntrack) in the Linux kernel. This flaw allows a remote user to disclose sensitive information via the DCCP protocol.
Severity: High
Risk Score: 7.5
EPSS Percentile: 10.6%

CVE-2022-48747

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: block: Fix wrong offset in bio_truncate() bio_truncate() clears the buffer outside of last block of bdev, however current bio_trun...
Severity: High
Risk Score: 7.5
EPSS Percentile: 37.9%

CVE-2022-43945

Component: Linux
Version: 3.10.108
Description: The Linux kernel NFSD implementation prior to versions 5.19.17 and 6.0.2 are vulnerable to buffer overflow. NFSD tracks the number of pages held by each NFSD thread by combining the receive and send b...
Severity: High
Risk Score: 7.5
EPSS Percentile: 64.1%

CVE-2022-36946 🔥 PoC

Reachable

Component: Linux
Version: 3.10.108
Description: nfqnl_mangle in net/netfilter/nfnetlink_queue.c in the Linux kernel through 5.18.14 allows remote attackers to cause a denial of service (panic) because, in the case of an nf_queue verdict with a one-...
Severity: High
Risk Score: 7.5
EPSS Percentile: 89.2%

CVE-2022-1199

Component: Linux
Version: 3.10.108
Description: A flaw was found in the Linux kernel. This flaw allows an attacker to crash the Linux kernel by simulating amateur radio from the user space, resulting in a null-ptr-deref vulnerability and a use-afte...
Severity: High
Risk Score: 7.5

EPSS Percentile: 33.8%

CVE-2021-45485

Unreachable

Component: Linux
Version: 3.10.108
Description: In the IPv6 implementation in the Linux kernel before 5.13.3, net/ipv6/output_core.c has an information leak because of certain use of a hash table which, although big, doesn't properly consider that ...
Severity: High
Risk Score: 7.5
EPSS Percentile: 58.5%

CVE-2021-38207

Unreachable

Component: Linux
Version: 3.10.108
Description: drivers/net/ethernet/xilinx/ll_temac_main.c in the Linux kernel before 5.12.13 allows remote attackers to cause a denial of service (buffer overflow and lockup) by sending heavy network traffic for ab...
Severity: High
Risk Score: 7.5
EPSS Percentile: 85.3%

CVE-2021-38202

Unreachable

Component: Linux
Version: 3.10.108
Description: fs/nfsd/trace.h in the Linux kernel before 5.13.4 might allow remote attackers to cause a denial of service (out-of-bounds read in strlen) by sending NFS traffic when the trace event framework is bein...
Severity: High
Risk Score: 7.5
EPSS Percentile: 84.8%

CVE-2020-25672

Component: Linux
Version: 3.10.108
Description: A memory leak vulnerability was found in Linux kernel in llcp_sock_connect
Severity: High
Risk Score: 7.5
EPSS Percentile: 82.6%

CVE-2020-25645 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A flaw was found in the Linux kernel in versions before 5.9-rc7. Traffic between two Geneve

endpoints may be unencrypted when IPsec is configured to encrypt traffic for the specific UDP port used by t...
Severity: High
Risk Score: 7.5
EPSS Percentile: 80.6%

CVE-2019-19074

Unreachable

Component: Linux
Version: 3.10.108
Description: A memory leak in the ath9k_wmi_cmd() function in drivers/net/wireless/ath/ath9k/wmi.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption), aka CID-728...
Severity: High
Risk Score: 7.5
EPSS Percentile: 69.8%

CVE-2019-19061

Unreachable

Component: Linux
Version: 3.10.108
Description: A memory leak in the adis_update_scan_mode_burst() function in drivers/iio/imu/adis_buffer.c in the Linux kernel before 5.3.9 allows attackers to cause a denial of service (memory consumption), aka CI...
Severity: High
Risk Score: 7.5
EPSS Percentile: 75.1%

CVE-2019-19060

Unreachable

Component: Linux
Version: 3.10.108
Description: A memory leak in the adis_update_scan_mode() function in drivers/iio/imu/adis_buffer.c in the Linux kernel before 5.3.9 allows attackers to cause a denial of service (memory consumption), aka CID-ab61...
Severity: High
Risk Score: 7.5
EPSS Percentile: 66.1%

CVE-2019-18807

Unreachable

Component: Linux
Version: 3.10.108
Description: Two memory leaks in the sja1105_static_config_upload() function in drivers/net/dsa/sja1105/sja1105_spi.c in the Linux kernel before 5.3.5 allow attackers to cause a denial of service (memory consumpti...
Severity: High
Risk Score: 7.5
EPSS Percentile: 77.9%

CVE-2019-17075

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in write_tpt_entry in drivers/infiniband/hw/cxgb4/mem.c in the Linux kernel through 5.3.2. The cxgb4 driver is directly calling dma_map_single (a DMA function) from a stack var...
Severity: High
Risk Score: 7.5
EPSS Percentile: 65.1%

CVE-2019-16921

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 4.17, hns_roce_alloc_ucontext in drivers/infiniband/hw/hns/hns_roce_main.c does not initialize the resp data structure, which might allow attackers to obtain sensitive infor...
Severity: High
Risk Score: 7.5
EPSS Percentile: 50.4%

CVE-2019-16714

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 5.2.14, rds6_inc_info_copy in net/rds/recv.c allows attackers to obtain sensitive information from kernel stack memory because tos and flags fields are not initialized.
Severity: High
Risk Score: 7.5
EPSS Percentile: 74.9%

CVE-2019-16413 🔥 PoC

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.0.4. The 9p filesystem did not protect i_size_write() properly, which causes an i_size_read() infinite loop and denial of service on SMP systems.
Severity: High
Risk Score: 7.5
EPSS Percentile: 79.7%

CVE-2019-15916

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.0.1. There is a memory leak in register_queue_kobjects() in net/core/net-sysfs.c, which will cause denial of service.
Severity: High
Risk Score: 7.5
EPSS Percentile: 85.0%

CVE-2019-12818

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 4.20.15. The nfc_llcp_build_tlv function in net/nfc/llcp_commands.c may return NULL. If the caller does not check for this, it will trigger a NULL po...
Severity: High
Risk Score: 7.5
EPSS Percentile: 89.9%

CVE-2019-12615

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in get_vdev_port_node_info in arch/sparc/kernel/mdesc.c in the Linux kernel through 5.1.6. There is an unchecked kstrdup_const of node_info->vdev_port.name, which might allow a...
Severity: High
Risk Score: 7.5
EPSS Percentile: 83.0%

CVE-2019-11810

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.0.7. A NULL pointer dereference can occur when megasas_create_frame_pool() fails in megasas_alloc_cmds() in drivers/scsi/megaraid/megaraid_sas_base...
Severity: High
Risk Score: 7.5
EPSS Percentile: 79.9%

CVE-2019-11478 🔥 PoC

Component: Linux
Version: 3.10.108
Description: Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences....
Severity: High
Risk Score: 7.5
EPSS Percentile: 99.6%

CVE-2019-11477 🔥 PoC

Component: Linux
Version: 3.10.108
Description: Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker co...
Severity: High
Risk Score: 7.5
EPSS Percentile: 99.7%

CVE-2018-6412

Unreachable

Component: Linux
Version: 3.10.108
Description: In the function sbusfb_ioctl_helper() in drivers/video/fbdev/sbuslib.c in the Linux kernel through 4.15, an integer signedness error allows arbitrary information leakage for the FBIOPUTCMAP_SPARC and ...
Severity: High
Risk Score: 7.5
EPSS Percentile: 48.8%

CVE-2018-5391 🔥 In VulnCheck KEV

Component: Linux
Version: 3.10.108
Description: The Linux kernel, versions 3.9+, is vulnerable to a denial of service attack with low rates of specially modified packets targeting IP fragment re-assembly. An attacker may cause a denial of service c...
Severity: High
Risk Score: 7.5
EPSS Percentile: 95.0%

CVE-2018-16871

Component: Linux
Version: 3.10.108
Description: A flaw was found in the Linux kernel's NFS implementation, all versions 3.x and all versions 4.x up to 4.20. An attacker, who is able to mount an exported NFS filesystem, is able to trigger a null poi...
Severity: High
Risk Score: 7.5
EPSS Percentile: 69.9%

CVE-2017-6214

Unreachable

Component: Linux
Version: 3.10.108
Description: The tcp_splice_read function in net/ipv4/tcp.c in the Linux kernel before 4.9.11 allows remote attackers to cause a denial of service (infinite loop and soft lockup) via vectors involving a TCP packet...
Severity: High

Risk Score: 7.5
EPSS Percentile: 90.6%

CVE-2017-5972 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The TCP stack in the Linux kernel 3.x does not properly implement a SYN cookie protection mechanism for the case of a fast network connection, which allows remote attackers to cause a denial of servic...
Severity: High
Risk Score: 7.5
EPSS Percentile: 95.3%

CVE-2017-5970

Unreachable

Component: Linux
Version: 3.10.108
Description: The ipv4_pktinfo_prepare function in net/ipv4/ip_sockglue.c in the Linux kernel through 4.9.9 allows attackers to cause a denial of service (system crash) via (1) an application that makes crafted sys...
Severity: High
Risk Score: 7.5
EPSS Percentile: 81.8%

CVE-2017-1000410

Component: Linux
Version: 3.10.108
Description: The Linux kernel version 3.3-rc1 and later is affected by a vulnerability lies in the processing of incoming L2CAP commands - ConfigRequest, and ConfigResponse messages. This info leak is a result of ...
Severity: High
Risk Score: 7.5
EPSS Percentile: 82.5%

CVE-2016-5244

Unreachable

Component: Linux
Version: 3.10.108
Description: The rds_inc_info_copy function in net/rds/recv.c in the Linux kernel through 4.6.3 does not initialize a certain structure member, which allows remote attackers to obtain sensitive information from ke...
Severity: High
Risk Score: 7.5
EPSS Percentile: 81.3%

CVE-2016-4580

Unreachable

Component: Linux
Version: 3.10.108
Description: The x25_negotiate_facilities function in net/x25/x25_facilities.c in the Linux kernel before 4.5.5 does not properly initialize a certain data structure, which allows attackers to obtain sensitive inf...
Severity: High
Risk Score: 7.5
EPSS Percentile: 70.7%

CVE-2016-4485

Unreachable

Component: Linux
Version: 3.10.108
Description: The llc_cmsg_rcv function in net/llc/af_llc.c in the Linux kernel before 4.5.5 does not initialize a certain data structure, which allows attackers to obtain sensitive information from kernel stack me...
Severity: High
Risk Score: 7.5
EPSS Percentile: 72.7%

CVE-2016-2117

Unreachable

Component: Linux
Version: 3.10.108
Description: The atl2_probe function in drivers/net/ethernet/atheros/atlx/atl2.c in the Linux kernel through 4.5.2 incorrectly enables scatter/gather I/O, which allows remote attackers to obtain sensitive informat...
Severity: High
Risk Score: 7.5
EPSS Percentile: 71.2%

CVE-2015-8746

Unreachable

Component: Linux
Version: 3.10.108
Description: fs/nfs/nfs4proc.c in the NFS client in the Linux kernel before 4.2.2 does not properly initialize memory for migration recovery operations, which allows remote NFS servers to cause a denial of service...
Severity: High
Risk Score: 7.5
EPSS Percentile: 82.3%

CVE-2014-4323

Component: Linux
Version: 3.10.108
Description: The mdp_lut_hw_update function in drivers/video/msm/mdp.c in the MDP display driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and oth...
Severity: High
Risk Score: 7.5

EPSS Percentile: 81.3%

CVE-2021-20322

Component: Linux
Version: 3.10.108
Description: A flaw in the processing of received ICMP errors (ICMP fragment needed and ICMP redirect) in the Linux kernel functionality was found to allow the ability to quickly scan open UDP ports. This flaw all...
Severity: High
Risk Score: 7.4
EPSS Percentile: 28.8%

CVE-2020-25705 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A flaw in ICMP packets in the Linux kernel may allow an attacker to quickly scan open UDP ports. This flaw allows an off-path remote attacker to effectively bypass source port UDP randomization. Softw...
Severity: High
Risk Score: 7.4
EPSS Percentile: 74.5%

CVE-2017-1000407

Component: Linux
Version: 3.10.108
Description: The Linux Kernel 2.6.32 and later are affected by a denial of service, by flooding the diagnostic port 0x80 an exception can be triggered leading to a kernel panic.
Severity: High
Risk Score: 7.4
EPSS Percentile: 63.1%

CVE-2017-1000364 🔥 Weaponized

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the size of the stack guard page on Linux, specifically a 4k stack guard page is not sufficiently large and can be "jumped" over (the stack guard page is bypassed), this aff...
Severity: High
Risk Score: 7.4
EPSS Percentile: 83.1%

CVE-2016-6516

Unreachable

Component: Linux
Version: 3.10.108
Description: Race condition in the ioctl_file_dedupe_range function in fs/ioctl.c in the Linux kernel through 4.7 allows local users to cause a denial of service (heap-based buffer overflow) or possibly gain privi...
Severity: High
Risk Score: 7.4

EPSS Percentile: 65.8%

CVE-2016-2069

Component: Linux
Version: 3.10.108
Description: Race condition in arch/x86/mm/tlb.c in the Linux kernel before 4.4.1 allows local users to gain privileges by triggering access to a paging structure by a different CPU.
Severity: High
Risk Score: 7.4
EPSS Percentile: 5.6%

CVE-2014-0049

Component: Linux
Version: 3.10.108
Description: Buffer overflow in the complete_emulated_mmio function in arch/x86/kvm/x86.c in the Linux kernel before 3.13.6 allows guest OS users to execute arbitrary code on the host OS by leveraging a loop that ...
Severity: High
Risk Score: 7.4
EPSS Percentile: 42.2%

CVE-2024-42093

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net/dpaa2: Avoid explicit cpumask var allocation on stack For CONFIG_CPUMASK_OFFSTACK=y kernel, explicit allocation of cpumask var...
Severity: High
Risk Score: 7.3
EPSS Percentile: 10.2%

CVE-2016-3841

Component: Linux
Version: 3.10.108
Description: The IPv6 stack in the Linux kernel before 4.3.3 mishandles options data, which allows local users to gain privileges or cause a denial of service (use-after-free and system crash) via a crafted sendms...
Severity: High
Risk Score: 7.3
EPSS Percentile: 9.9%

CVE-2015-8955

Component: Linux
Version: 3.10.108
Description: arch/arm64/kernel/perf_event.c in the Linux kernel before 4.1 on arm64 platforms allows local users to gain privileges or cause a denial of service (invalid pointer dereference) via vectors involving ...
Severity: High
Risk Score: 7.3

EPSS Percentile: 23.5%

CVE-2020-25643

Component: Linux
Version: 3.10.108
Description: A flaw was found in the HDLC_PPP module of the Linux kernel in versions before 5.9-rc7. Memory corruption and a read overflow is caused by improper input validation in the ppp_cp_parse_cr function whi...
Severity: High
Risk Score: 7.2
EPSS Percentile: 59.5%

CVE-2015-5157

Unreachable

Component: Linux
Version: 3.10.108
Description: arch/x86/entry/entry_64.S in the Linux kernel before 4.1.6 on the x86_64 platform mishandles IRET faults in processing NMIs that occurred during userspace execution, which might allow local users to g...
Severity: High
Risk Score: 7.2
EPSS Percentile: 46.0%

CVE-2015-3290 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: arch/x86/entry/entry_64.S in the Linux kernel before 4.1.6 on the x86_64 platform improperly relies on espfix64 during nested NMI processing, which allows local users to gain privileges by triggering ...
Severity: High
Risk Score: 7.2
EPSS Percentile: 75.2%

CVE-2015-1805 🔥 In VulnCheck KEV

Unreachable

Component: Linux
Version: 3.10.108
Description: The (1) pipe_read and (2) pipe_write implementations in fs/pipe.c in the Linux kernel before 3.16 do not properly consider the side effects of failed __copy_to_user_inatomic and __copy_from_user_inato...
Severity: High
Risk Score: 7.2
EPSS Percentile: 91.9%

CVE-2014-7822 🔥 PoC

Component: Linux
Version: 3.10.108

Description: The implementation of certain splice_write file operations in the Linux kernel before 3.16 does not enforce a restriction on the maximum size of a single file, which allows local users to cause a deni...
Severity: High
Risk Score: 7.2
EPSS Percentile: 70.7%

CVE-2014-4322 🔥 PoC

Component: Linux
Version: 3.10.108
Description: drivers/misc/qseecom.c in the QSEECOM driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, does not validate certain ...
Severity: High
Risk Score: 7.2
EPSS Percentile: 87.0%

CVE-2025-37785

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ext4: fix OOB read when checking dotdot dir Mounting a corrupted filesystem with directory which contains '.' dir entry with rec_l...
Severity: High
Risk Score: 7.1
EPSS Percentile: 3.7%

CVE-2025-22038

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate zero num_subauth before sub_auth is accessed Access psid->sub_auth[psid->num_subauth - 1] without checking if num_...
Severity: High
Risk Score: 7.1
EPSS Percentile: 2.7%

CVE-2025-21993

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: iscsi_ibft: Fix UBSAN shift-out-of-bounds warning in ibft_attr_show_nic() When performing an iSCSI boot using IPv6, iscsistart sti...
Severity: High
Risk Score: 7.1
EPSS Percentile: 4.0%

CVE-2025-21920

Reachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: vlan: enforce underlying device type Currently, VLAN devices can be created on top of non-ethernet devices. Besides the fact that...
Severity: High
Risk Score: 7.1
EPSS Percentile: 4.0%

CVE-2025-21782

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: orangefs: fix a oob in orangefs_debug_write I got a syzbot report: slab-out-of-bounds Read in orangefs_debug_write... several peop...
Severity: High
Risk Score: 7.1
EPSS Percentile: 10.3%

CVE-2024-56650

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: netfilter: x_tables: fix LED ID check in led_tg_check() Syzbot has reported the following BUG detected by KASAN: BUG: KASAN: slab...
Severity: High
Risk Score: 7.1
EPSS Percentile: 7.7%

CVE-2024-53155

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix uninitialized value in ocfs2_file_read_iter() Syzbot has reported the following KMSAN splat: BUG: KMSAN: uninit-value ...
Severity: High
Risk Score: 7.1
EPSS Percentile: 8.9%

CVE-2024-53150 🔥 In VulnCheck KEV

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: Fix out of bounds reads when finding clock sources The current USB-audio driver code doesn't check bLength of eac...
Severity: High
Risk Score: 7.1
EPSS Percentile: 37.3%

CVE-2024-53108

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Adjust VSDB parser for replay feature At some point, the IEEE ID identification for the replay check in the AMD E...
Severity: High
Risk Score: 7.1
EPSS Percentile: 5.3%

CVE-2024-53099

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: bpf: Check validity of link->type in bpf_link_show_fdinfo() If a newly-added link type doesn't invoke BPF_LINK_TYPE(), accessing b...
Severity: High
Risk Score: 7.1
EPSS Percentile: 6.6%

CVE-2024-50247

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: Check if more than chunk-size bytes are written A incorrectly formatted chunk may decompress into more than LZNT_CHUNK_S...
Severity: High
Risk Score: 7.1
EPSS Percentile: 19.0%

CVE-2024-50193

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: x86/entry_32: Clear CPU buffers after register restore in NMI return CPU buffers are currently cleared after call to exc_nmi, but ...
Severity: High
Risk Score: 7.1
EPSS Percentile: 6.8%

CVE-2024-50115

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: KVM: nSVM: Ignore nCR3[4:0] when loading PDPTEs from memory Ignore nCR3[4:0] when loading PDPTEs from memory for nested SVM, as bi...
Severity: High
Risk Score: 7.1
EPSS Percentile: 13.0%

CVE-2024-50035

Reachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ppp: fix ppp_async_encode() illegal access syzbot reported an issue in ppp_async_encode() [1] In this case, pppoe_sendmsg() is ca...
Severity: High
Risk Score: 7.1
EPSS Percentile: 8.8%

CVE-2024-50033

Reachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: slip: make slhc_remember() more robust against malicious packets syzbot found that slhc_remember() was missing checks against mali...
Severity: High
Risk Score: 7.1
EPSS Percentile: 13.8%

CVE-2024-49928

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: wifi: rtw89: avoid reading out of bounds when loading TX power FW elements Because the loop-expression will do one more time befor...
Severity: High
Risk Score: 7.1
EPSS Percentile: 7.1%

CVE-2024-49900

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: jfs: Fix uninit-value access of new_ea in ea_buffer syzbot reports that lzo1x_1_do_compress is using uninit-value: ==========...
Severity: High
Risk Score: 7.1
EPSS Percentile: 8.0%

CVE-2024-49860

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ACPI: sysfs: validate return type of _STR method Only buffer objects are valid return values of _STR. If something else is return...
Severity: High
Risk Score: 7.1
EPSS Percentile: 12.5%

CVE-2024-47757

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix potential oob read in nilfs_btree_check_delete() The function nilfs_btree_check_delete(), which checks whether degener...
Severity: High
Risk Score: 7.1
EPSS Percentile: 12.5%

CVE-2024-47723

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: jfs: fix out-of-bounds in dbNextAG() and diAlloc() In dbNextAG() , there is no check for the case where bmp->db_numag is greater o...
Severity: High
Risk Score: 7.1
EPSS Percentile: 8.0%

CVE-2024-46774

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: powerpc/rtas: Prevent Spectre v1 gadget construction in sys_rtas() Smatch warns: arch/powerpc/kernel/rtas.c:1932 __do_sys_rtas(...
Severity: High

Risk Score: 7.1
EPSS Percentile: 29.8%

CVE-2024-46747

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: HID: cougar: fix slab-out-of-bounds Read in cougar_report_fixup report_fixup for the Cougar 500k Gaming Keyboard was not verifying...
Severity: High
Risk Score: 7.1
EPSS Percentile: 13.9%

CVE-2024-46743

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: of/irq: Prevent device address out-of-bounds read in interrupt map walk When of_irq_parse_raw() is invoked with a device address s...
Severity: High
Risk Score: 7.1
EPSS Percentile: 13.9%

CVE-2024-46731

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amd/pm: fix the Out-of-bounds read warning using index i - 1U may beyond element index for mc_data[] when i = 0.
Severity: High
Risk Score: 7.1
EPSS Percentile: 9.9%

CVE-2024-46724

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix out-of-bounds read of df_v1_7_channel_number Check the fb_channel_number range to avoid the array out-of-bounds re...
Severity: High
Risk Score: 7.1
EPSS Percentile: 9.9%

CVE-2024-46723

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix ucode out-of-bounds read warning Clear warning that read ucode[] may out-of-bounds.
Severity: High
Risk Score: 7.1
EPSS Percentile: 13.9%

CVE-2024-46722

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix mc_data out-of-bounds read warning Clear warning that read mc_data[i-1] may out-of-bounds.
Severity: High
Risk Score: 7.1
EPSS Percentile: 13.9%

CVE-2024-42094

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net/iucv: Avoid explicit cpumask var allocation on stack For CONFIG_CPUMASK_OFFSTACK=y kernel, explicit allocation of cpumask vari...
Severity: High
Risk Score: 7.1
EPSS Percentile: 10.5%

CVE-2024-41059

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: hfsplus: fix uninit-value in copy_name [syzbot reported] BUG: KMSAN: uninit-value in sized_strscpy+0xc4/0x160 sized_strscpy+0xc4/...
Severity: High
Risk Score: 7.1
EPSS Percentile: 10.3%

CVE-2024-41014

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: xfs: add bounds checking to

xlog_recover_process_data There is a lack of verification of the space occupied by fixed members of xl...
Severity: High
Risk Score: 7.1
EPSS Percentile: 10.0%

CVE-2024-39471

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: add error handle to avoid out-of-bounds if the sdma_v4_0_irq_id_to_seq return -EINVAL, the process should be stop to a...
Severity: High
Risk Score: 7.1
EPSS Percentile: 10.3%

CVE-2024-38538

Reachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net: bridge: xmit: make sure we have at least eth header len bytes syzbot triggered an uninit value[1] error in bridge device's xm...
Severity: High
Risk Score: 7.1
EPSS Percentile: 9.7%

CVE-2024-36960

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: Fix invalid reads in fence signaled events Correctly set the length of the drm_event to the size of the structure that...
Severity: High
Risk Score: 7.1
EPSS Percentile: 1.5%

CVE-2024-35937

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: wifi: cfg80211: check A-MSDU format more carefully If it looks like there's another subframe in the A-MSDU but the header isn't fu...
Severity: High
Risk Score: 7.1
EPSS Percentile: 2.5%

CVE-2024-35896

Reachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: netfilter: validate user input for expected length I got multiple syzbot reports showing old bugs exposed by BPF after commit 20f2...
Severity: High
Risk Score: 7.1
EPSS Percentile: 1.3%

CVE-2024-35849

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: btrfs: fix information leak in btrfs_ioctl_logical_to_ino() Syzbot reported the following information leak for in btrfs_ioctl_logi...
Severity: High
Risk Score: 7.1
EPSS Percentile: 2.5%

CVE-2024-26982

Reachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: Squashfs: check the inode number is not the invalid value of zero Syskiller has produced an out of bounds access in fill_meta_inde...
Severity: High
Risk Score: 7.1
EPSS Percentile: 12.6%

CVE-2024-26791

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: btrfs: dev-replace: properly validate device names There's a syzbot report that device name buffers passed to device replace are n...
Severity: High
Risk Score: 7.1
EPSS Percentile: 0.3%

CVE-2024-26763

Unreachable

Component: Linux
Version: 3.10.108

Description: In the Linux kernel, the following vulnerability has been resolved: dm-crypt: don't modify the data when using authenticated encryption It was said that authenticated encryption could produce invali...
Severity: High
Risk Score: 7.1
EPSS Percentile: 1.7%

CVE-2024-26672

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix variable 'mca_funcs' dereferenced before NULL check in 'amdgpu_mca_smu_get_mca_entry()' Fixes the below: drivers/...
Severity: High
Risk Score: 7.1
EPSS Percentile: 1.1%

CVE-2024-26594

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate mech token in session setup If client send invalid mech token in session setup request, ksmbd validate and make th...
Severity: High
Risk Score: 7.1
EPSS Percentile: 62.3%

CVE-2024-0775

Unreachable

Component: Linux
Version: 3.10.108
Description: A use-after-free flaw was found in the __ext4_remount in fs/ext4/super.c in ext4 in the Linux kernel. This flaw allows a local user to cause an information leak problem while freeing the old quota fil...
Severity: High
Risk Score: 7.1
EPSS Percentile: 0.6%

CVE-2023-52827

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: fix possible out-of-bound read in ath12k_htt_pull_ppdu_stats() len is extracted from HTT message and could be an une...
Severity: High
Risk Score: 7.1

EPSS Percentile: 1.4%

CVE-2023-52766

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: i3c: mipi-i3c-hci: Fix out of bounds access in hci_dma_irq_handler Do not loop over ring headers in hci_dma_irq_handler() that are...
Severity: High
Risk Score: 7.1
EPSS Percentile: 10.1%

CVE-2023-52640

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: Fix oob in ntfs_listxattr The length of name cannot exceed the space occupied by ea.
Severity: High
Risk Score: 7.1
EPSS Percentile: 6.2%

CVE-2023-52598

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: s390/ptrace: handle setting of fpc register correctly If the content of the floating point control (fpc) register of a traced proc...
Severity: High
Risk Score: 7.1
EPSS Percentile: 0.4%

CVE-2023-52588

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to tag gcing flag on page during block migration It needs to add missing gcing flag on page during block migration, in o...
Severity: High
Risk Score: 7.1
EPSS Percentile: 1.1%

CVE-2023-52507

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: nfc: nci: assert requested protocol is valid The protocol is used in a bit mask to determine if the protocol is supported. Assert ...
Severity: High
Risk Score: 7.1
EPSS Percentile: 0.3%

CVE-2023-52501

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ring-buffer: Do not attempt to read past "commit" When iterating over the ring buffer while the ring buffer is active, the writer ...
Severity: High
Risk Score: 7.1
EPSS Percentile: 7.1%

CVE-2023-52479

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix uaf in smb20_oplock_break_ack drop reference after use opinfo.
Severity: High
Risk Score: 7.1
EPSS Percentile: 2.9%

CVE-2023-3567

Unreachable

Component: Linux
Version: 3.10.108
Description: A use-after-free flaw was found in vcs_read in drivers/tty/vt/vc_screen.c in vc_screen in the Linux Kernel. This issue may allow an attacker with local user access to cause a system crash or leak inte...
Severity: High
Risk Score: 7.1
EPSS Percentile: 0.5%

CVE-2023-3268

Unreachable

Component: Linux
Version: 3.10.108
Description: An out of bounds (OOB) memory access flaw was found in the Linux kernel in relay_file_read_start_pos in kernel/relay.c in the relayfs. This flaw could allow a local attacker to crash the system or lea...

Severity: High
Risk Score: 7.1
EPSS Percentile: 0.3%

CVE-2023-3141

Unreachable

Component: Linux
Version: 3.10.108
Description: A use-after-free flaw was found in r592_remove in drivers/memstick/host/r592.c in media access in the Linux Kernel. This flaw allows a local attacker to crash the system at device disconnect, possibly...
Severity: High
Risk Score: 7.1
EPSS Percentile: 0.4%

CVE-2023-26607 🔥 PoC

Component: Linux
Version: 3.10.108
Description: In the Linux kernel 6.0.8, there is an out-of-bounds read in ntfs_attr_find in fs/ntfs/attrib.c.
Severity: High
Risk Score: 7.1
EPSS Percentile: 33.5%

CVE-2023-1380

Unreachable

Component: Linux
Version: 3.10.108
Description: A slab-out-of-bound read problem was found in brcmf_get_assoc_ies in drivers/net/wireless/broadcom/brcm80211/brcmfmac/cfg80211.c in the Linux Kernel. This issue could occur when assoc_info->req_len da...
Severity: High
Risk Score: 7.1
EPSS Percentile: 2.7%

CVE-2022-49740

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: wifi: brcmfmac: Check the count value of channel spec to prevent out-of-bounds reads This patch fixes slab-out-of-bounds reads in ...
Severity: High
Risk Score: 7.1
EPSS Percentile: 2.1%

CVE-2022-49738

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to do sanity check on i_extra_isize in is_alive() syzbot found a f2fs bug: BUG: KASAN: slab-out-of-bounds in data_blkad...
Severity: High
Risk Score: 7.1
EPSS Percentile: 2.8%

CVE-2022-49623

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: powerpc/xive/spapr: correct bitmap allocation size kasan detects access beyond the end of the xibm->bitmap allocation: BUG: KASAN...
Severity: High
Risk Score: 7.1
EPSS Percentile: 6.2%

CVE-2022-49395

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: um: Fix out-of-bounds read in LDT setup syscall_stub_data() expects the data_count parameter to be the number of longs, not bytes....
Severity: High
Risk Score: 7.1
EPSS Percentile: 5.9%

CVE-2022-48967

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: NFC: nci: Bounds check struct nfc_target arrays While running under CONFIG_FORTIFY_SOURCE=y, syzkaller reported: memcpy: detect...
Severity: High
Risk Score: 7.1
EPSS Percentile: 8.0%

CVE-2022-48739

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ASoC: hdmi-codec: Fix OOB memory accesses Correct size of iec_status array by changing it to the size of status array of the struc...
Severity: High

Risk Score: 7.1
EPSS Percentile: 19.3%

CVE-2022-48701

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: Fix an out-of-bounds bug in __snd_usb_parse_audio_interface() There may be a bad USB audio device with a USB ID o...
Severity: High
Risk Score: 7.1
EPSS Percentile: 0.7%

CVE-2022-41858

Unreachable

Component: Linux
Version: 3.10.108
Description: A flaw was found in the Linux kernel. A NULL pointer dereference may occur while a slip driver is in progress to detach in sl_tx_timeout in drivers/net/slip/slip.c. This issue could allow an attacker ...
Severity: High
Risk Score: 7.1
EPSS Percentile: 0.7%

CVE-2022-3564

Unreachable

Component: Linux
Version: 3.10.108
Description: A vulnerability classified as critical was found in Linux Kernel. Affected by this vulnerability is the function l2cap_reassemble_sdu of the file net/bluetooth/l2cap_core.c of the component Bluetooth....
Severity: High
Risk Score: 7.1
EPSS Percentile: 20.5%

CVE-2022-33742

Component: Linux
Version: 3.10.108
Description: Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Linux Block and Network PV device f...
Severity: High
Risk Score: 7.1
EPSS Percentile: 5.8%

CVE-2022-33741

Component: Linux
Version: 3.10.108
Description: Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Linux Block and Network PV device f...
Severity: High
Risk Score: 7.1
EPSS Percentile: 8.1%

CVE-2022-33740

Component: Linux
Version: 3.10.108
Description: Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Linux Block and Network PV device f...
Severity: High
Risk Score: 7.1
EPSS Percentile: 11.1%

CVE-2022-3202

Unreachable

Component: Linux
Version: 3.10.108
Description: A NULL pointer dereference flaw in diFree in fs/jfs/inode.c in Journaled File System (JFS)in the Linux kernel. This could allow a local attacker to crash the system or leak kernel internal information...
Severity: High
Risk Score: 7.1
EPSS Percentile: 3.0%

CVE-2022-26365

Component: Linux
Version: 3.10.108
Description: Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Linux Block and Network PV device f...
Severity: High
Risk Score: 7.1
EPSS Percentile: 8.1%

CVE-2022-1353

Reachable

Component: Linux
Version: 3.10.108
Description: A vulnerability was found in the pfkey_register function in net/key/af_key.c in the Linux kernel. This flaw allows a local, unprivileged user to gain access to kernel memory, leading to a system crash...
Severity: High
Risk Score: 7.1
EPSS Percentile: 1.1%

CVE-2022-0850 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A vulnerability was found in linux kernel, where an information leak occurs via ext4_extent_header to userspace.
Severity: High
Risk Score: 7.1
EPSS Percentile: 29.9%

CVE-2021-47636

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ubifs: Fix read out-of-bounds in ubifs_wbuf_write_nolock() Function ubifs_wbuf_write_nolock() may access buf out of bounds in foll...
Severity: High
Risk Score: 7.1
EPSS Percentile: 6.5%

CVE-2021-47624

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net/sunrpc: fix reference count leaks in rpc_sysfs_xprt_state_change The refcount leak issues take place in an error handling path...
Severity: High
Risk Score: 7.1
EPSS Percentile: 7.6%

CVE-2021-47327

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: iommu/arm-smmu: Fix arm_smmu_device refcount leak when arm_smmu_rpm_get fails arm_smmu_rpm_get() invokes pm_runtime_get_sync(), wh...
Severity: High
Risk Score: 7.1
EPSS Percentile: 14.6%

CVE-2021-47288

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: media: ngene: Fix out-of-bounds

bug in ngene_command_config_free_buf() Fix an 11-year old bug in ngene_command_config_free_buf() w...
Severity: High
Risk Score: 7.1
EPSS Percentile: 12.1%

CVE-2021-47277

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: kvm: avoid speculation-based attacks from out-of-range memslot accesses KVM's mechanism for accessing guest memory translates a gu...
Severity: High
Risk Score: 7.1
EPSS Percentile: 1.0%

CVE-2021-47219

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: scsi: scsi_debug: Fix out-of-bound read in resp_report_tgtpgs() The following issue was observed running syzkaller: BUG: KASAN: s...
Severity: High
Risk Score: 7.1
EPSS Percentile: 0.6%

CVE-2021-47191

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: scsi: scsi_debug: Fix out-of-bound read in resp_readcap16() The following warning was observed running syzkaller: [3813.830724] ...
Severity: High
Risk Score: 7.1
EPSS Percentile: 0.6%

CVE-2021-47110

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: x86/kvm: Disable kvmclock on all CPUs on shutdown Currenly, we disable kvmclock from machine_shutdown() hook and this only happens...
Severity: High
Risk Score: 7.1
EPSS Percentile: 0.9%

CVE-2021-47083

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: pinctrl: mediatek: fix global-out-of-bounds issue When eint virtual eint number is greater than gpio number, it maybe produce 'des...
Severity: High
Risk Score: 7.1
EPSS Percentile: 0.6%

CVE-2021-4204 🔥 PoC

Component: Linux
Version: 3.10.108
Description: An out-of-bounds (OOB) memory access flaw was found in the Linux kernel's eBPF due to an Improper Input Validation. This flaw allows a local attacker with a special privilege to crash the system or le...
Severity: High
Risk Score: 7.1
EPSS Percentile: 71.2%

CVE-2021-4090

Unreachable

Component: Linux
Version: 3.10.108
Description: An out-of-bounds (OOB) memory write flaw was found in the NFSD in the Linux kernel. Missing sanity may lead to a write beyond bmval[bmlen-1] in nfsd4_decode_bitmap4 in fs/nfsd/nfs4xdr.c. In this flaw,...
Severity: High
Risk Score: 7.1
EPSS Percentile: 12.0%

CVE-2021-3752 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A use-after-free flaw was found in the Linux kernel’s Bluetooth subsystem in the way user calls connect to the socket and disconnect simultaneously due to a race condition. This flaw allows a user to ...
Severity: High
Risk Score: 7.1
EPSS Percentile: 47.3%

CVE-2021-3739 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: A NULL pointer dereference flaw was found in the btrfs_rm_device function in fs/btrfs/volumes.c in the Linux Kernel, where triggering the bug requires ‘CAP_SYS_ADMIN’. This flaw allows a local attacke...
Severity: High
Risk Score: 7.1
EPSS Percentile: 5.1%

CVE-2021-3506

Unreachable

Component: Linux
Version: 3.10.108
Description: An out-of-bounds (OOB) memory access flaw was found in fs/f2fs/node.c in the f2fs module in the Linux kernel in versions before 5.12.0-rc4. A bounds check failure allows a local attacker to gain acces...
Severity: High
Risk Score: 7.1
EPSS Percentile: 58.0%

CVE-2021-3501

Component: Linux
Version: 3.10.108
Description: A flaw was found in the Linux kernel in versions before 5.12. The value of internal.ndata, in the KVM API, is mapped to an array index, which can be updated by a user process at anytime which could le...
Severity: High
Risk Score: 7.1
EPSS Percentile: 10.8%

CVE-2021-32078 🔥 PoC

Component: Linux
Version: 3.10.108
Description: An Out-of-Bounds Read was discovered in arch/arm/mach-footbridge/personal-pci.c in the Linux kernel through 5.12.11 because of the lack of a check for a value that shouldn't be negative, e.g., access ...
Severity: High
Risk Score: 7.1
EPSS Percentile: 37.0%

CVE-2021-27364 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 5.11.3. drivers/scsi/scsi_transport_iscsi.c is adversely affected by the ability of an unprivileged user to craft Netlink messages.
Severity: High
Risk Score: 7.1
EPSS Percentile: 41.9%

CVE-2020-8648 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the n_tty_receive_buf_common function in drivers/tty/n_tty.c.

Severity: High
Risk Score: 7.1
EPSS Percentile: 45.1%

CVE-2020-36386 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.8.1. net/bluetooth/hci_event.c has a slab out-of-bounds read in hci_extended_inquiry_result_evt, aka CID-51c19bf3d5cf.
Severity: High
Risk Score: 7.1
EPSS Percentile: 28.7%

CVE-2020-24394

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 5.7.8, fs/nfsd/vfs.c (in the NFS server) can set incorrect permissions on new filesystem objects when the filesystem lacks ACL support, aka CID-22cf8419f131. This occurs bec...
Severity: High
Risk Score: 7.1
EPSS Percentile: 2.2%

CVE-2020-12654

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was found in Linux kernel before 5.5.4. mwifiex_ret_wmm_get_status() in drivers/net/wireless/marvell/mwifiex/wmm.c allows a remote AP to trigger a heap-based buffer overflow because of an inc...
Severity: High
Risk Score: 7.1
EPSS Percentile: 27.8%

CVE-2020-11668

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 5.6.1, drivers/media/usb/gspca/xirlink_cit.c (aka the Xirlink camera USB driver) mishandles invalid descriptors, aka CID-a246b4d54770.
Severity: High
Risk Score: 7.1
EPSS Percentile: 11.6%

CVE-2019-25160

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: netlabel: fix out-of-bounds memory accesses There are two array out-of-bounds memory accesses, one in cipso_v4_map_lvl_valid(), th...
Severity: High
Risk Score: 7.1
EPSS Percentile: 1.3%

CVE-2018-18021

Unreachable

Component: Linux
Version: 3.10.108
Description: arch/arm64/kvm/guest.c in KVM in the Linux kernel before 4.18.12 on the arm64 platform mishandles the KVM_SET_ON_REG ioctl. This is exploitable by attackers who can create virtual machines. An attacke...
Severity: High
Risk Score: 7.1
EPSS Percentile: 26.9%

CVE-2017-7277

Unreachable

Component: Linux
Version: 3.10.108
Description: The TCP stack in the Linux kernel through 4.10.6 mishandles the SCM_TIMESTAMPING_OPT_STATS feature, which allows local users to obtain sensitive information from the kernel's internal socket data stru...
Severity: High
Risk Score: 7.1
EPSS Percentile: 13.2%

CVE-2017-2584

Component: Linux
Version: 3.10.108
Description: arch/x86/kvm/emulate.c in the Linux kernel through 4.9.3 allows local users to obtain sensitive information from kernel memory or cause a denial of service (use-after-free) via a crafted application t...
Severity: High
Risk Score: 7.1
EPSS Percentile: 26.2%

CVE-2017-18270

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 4.13.5, a local user could create keyrings for other users via keyctl

commands, setting unwanted defaults or causing a denial of service.
Severity: High
Risk Score: 7.1
EPSS Percentile: 2.3%

CVE-2017-12154

Component: Linux
Version: 3.10.108
Description: The prepare_vmcs02 function in arch/x86/kvm/vmx.c in the Linux kernel through 4.13.3 does not ensure that the "CR8-load exiting" and "CR8-store exiting" L0 vmcs02 controls exist in cases where L1 omit...
Severity: High
Risk Score: 7.1
EPSS Percentile: 17.9%

CVE-2017-11472

Unreachable

Component: Linux
Version: 3.10.108
Description: The acpi_ns_terminate() function in drivers/acpi/acpica/nsutils.c in the Linux kernel before 4.12 does not flush the operand cache and causes a kernel stack dump, which allows local users to obtain se...
Severity: High
Risk Score: 7.1
EPSS Percentile: 17.3%

CVE-2016-4998 🔥 Weaponized

Component: Linux
Version: 3.10.108
Description: The IPT_SO_SET_REPLACE setsockopt implementation in the netfilter subsystem in the Linux kernel before 4.6 allows local users to cause a denial of service (out-of-bounds read) or possibly obtain sensi...
Severity: High
Risk Score: 7.1
EPSS Percentile: 78.3%

CVE-2016-3713

Component: Linux
Version: 3.10.108
Description: The msr_mtrr_valid function in arch/x86/kvm/mtrr.c in the Linux kernel before 4.6.1 supports MSR 0x2f8, which allows guest OS users to read or write to the kvm_arch_vcpu data structure, and consequent...
Severity: High
Risk Score: 7.1
EPSS Percentile: 28.0%

CVE-2025-21718

Unreachable

Component: Linux
Version: 3.10.108

Description: In the Linux kernel, the following vulnerability has been resolved: net: rose: fix timer races against user threads Rose timers only acquire the socket spinlock, without checking if the socket is ow...
Severity: High
Risk Score: 7.0
EPSS Percentile: 5.9%

CVE-2024-50286

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix slab-use-after-free in ksmbd_smb2_session_create There is a race condition between ksmbd_smb2_session_create and ksmbd_...
Severity: High
Risk Score: 7.0
EPSS Percentile: 7.4%

CVE-2024-50234

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: wifi: iwlegacy: Clear stale interrupts before resuming device iwl4965 fails upon resume from hibernation on my laptop. The reason ...
Severity: High
Risk Score: 7.0
EPSS Percentile: 6.2%

CVE-2024-50086

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix user-after-free from session log off There is racy issue between smb2 session log off and smb2 session setup. It will c...
Severity: High
Risk Score: 7.0
EPSS Percentile: 7.3%

CVE-2024-50061

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: i3c: master: cdns: Fix use after free vulnerability in cdns_i3c_master Driver Due to Race Condition In the cdns_i3c_master_probe f...
Severity: High
Risk Score: 7.0

EPSS Percentile: 9.7%

CVE-2024-50059

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ntb: ntb_hw_switchtec: Fix use after free vulnerability in switchtec_ntb_remove due to race condition In the switchtec_ntb_add fun...
Severity: High
Risk Score: 7.0
EPSS Percentile: 8.8%

CVE-2024-50036

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net: do not delay dst_entries_add() in dst_release() dst_entries_add() uses per-cpu data that might be freed at netns dismantle fr...
Severity: High
Risk Score: 7.0
EPSS Percentile: 13.2%

CVE-2024-49903

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: jfs: Fix uaf in dbFreeBits [syzbot reported] == BUG: KASAN: slab-u...
Severity: High
Risk Score: 7.0
EPSS Percentile: 8.0%

CVE-2024-43882

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: exec: Fix ToCToU between perm check and set-uid/gid usage When opening a file for exec via do_filp_open(), permission checking is ...
Severity: High
Risk Score: 7.0
EPSS Percentile: 15.5%

CVE-2024-42228

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Using uninitialized value *size when calling amdgpu_vce_cs_reloc Initialize the size before calling amdgpu_vce_cs_relo...
Severity: High
Risk Score: 7.0
EPSS Percentile: 9.9%

CVE-2024-26976

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: KVM: Always flush async #PF workqueue when vCPU is being destroyed Always flush the per-vCPU async #PF workqueue when a vCPU is cl...
Severity: High
Risk Score: 7.0
EPSS Percentile: 0.3%

CVE-2024-26872

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: RDMA/srpt: Do not register event handler until srpt device is fully setup Upon rare occasions, KASAN reports a use-after-free Writ...
Severity: High
Risk Score: 7.0
EPSS Percentile: 1.3%

CVE-2024-26654

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ALSA: sh: aica: reorder cleanup operations to avoid UAF bugs The dreamcastcard->timer could schedule the spu_dma_work and the spu_...
Severity: High
Risk Score: 7.0
EPSS Percentile: 1.2%

CVE-2023-6932 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: A use-after-free vulnerability in the Linux kernel's ipv4: igmp component can be exploited to achieve local privilege escalation. A race condition can be exploited to cause a timer be mistakenly regi...
Severity: High

Risk Score: 7.0
EPSS Percentile: 5.8%

CVE-2023-6546 🔥 Commercial Exploit

Unreachable

Component: Linux
Version: 3.10.108
Description: A race condition was found in the GSM 0710 tty multiplexor in the Linux kernel. This issue occurs when two threads execute the GSMIOC_SETCONF ioctl on the same tty file descriptor with the gsm line di...
Severity: High
Risk Score: 7.0
EPSS Percentile: 49.9%

CVE-2023-6531 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A use-after-free flaw was found in the Linux Kernel due to a race problem in the unix garbage collector's deletion of SKB races with unix_stream_read_generic() on the socket that the SKB is queued on.
Severity: High
Risk Score: 7.0
EPSS Percentile: 5.1%

CVE-2023-6270

Unreachable

Component: Linux
Version: 3.10.108
Description: A flaw was found in the ATA over Ethernet (AoE) driver in the Linux kernel. The aoecmd_cfg_pkts() function improperly updates the refcnt on `struct net_device`, and a use-after-free can be triggered b...
Severity: High
Risk Score: 7.0
EPSS Percentile: 3.9%

CVE-2023-52586

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm/msm/dpu: Add mutex lock in control vblank irq Add a mutex lock to control vblank irq to synchronize vblank enable/disable oper...
Severity: High
Risk Score: 7.0
EPSS Percentile: 0.9%

CVE-2023-52578

Reachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net: bridge: use DEV_STATS_INC() syzbot/KCSAN reported data-races in br_handle_frame_finish() [1] This function can run from multi...
Severity: High
Risk Score: 7.0
EPSS Percentile: 0.5%

CVE-2023-52517

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: spi: sun6i: fix race between DMA RX transfer completion and RX FIFO drain Previously the transfer complete IRQ immediately drained...
Severity: High
Risk Score: 7.0
EPSS Percentile: 0.8%

CVE-2023-51782

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 6.6.8. rose_ioctl in net/rose/af_rose.c has a use-after-free because of a rose_accept race condition.
Severity: High
Risk Score: 7.0
EPSS Percentile: 3.0%

CVE-2023-51781

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 6.6.8. atalk_ioctl in net/appletalk/ddp.c has a use-after-free because of an atalk_recvmsg race condition.
Severity: High
Risk Score: 7.0
EPSS Percentile: 2.7%

CVE-2023-51780

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 6.6.8. do_vcc_ioctl in net/atm/ioctl.c has a use-after-free because of a vcc_recvmsg race condition.
Severity: High

Risk Score: 7.0
EPSS Percentile: 3.9%

CVE-2023-51043

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 6.4.5, drivers/gpu/drm/drm_atomic.c has a use-after-free during a race condition between a nonblocking atomic commit and a driver unload.
Severity: High
Risk Score: 7.0
EPSS Percentile: 0.8%

CVE-2023-46813 🔥 PoC

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 6.5.9, exploitable by local users with userspace access to MMIO registers. Incorrect access checking in the #VC handler and instruction emulation of ...
Severity: High
Risk Score: 7.0
EPSS Percentile: 35.5%

CVE-2023-4244 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. Due to a race condition between nf_tables netlink control p...
Severity: High
Risk Score: 7.0
EPSS Percentile: 3.1%

CVE-2023-35827

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 6.3.8. A use-after-free was found in ravb_remove in drivers/net/ethernet/renesas/ravb_main.c.
Severity: High
Risk Score: 7.0
EPSS Percentile: 1.1%

CVE-2023-35824

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in dm1105_remove in drivers/media/pci/dm1105/dm1105.c.
Severity: High
Risk Score: 7.0
EPSS Percentile: 0.8%

CVE-2023-35823

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in saa7134_finidev in drivers/media/pci/saa7134/saa7134-core.c.
Severity: High
Risk Score: 7.0
EPSS Percentile: 1.3%

CVE-2023-1989

Component: Linux
Version: 3.10.108
Description: A use-after-free flaw was found in btsdio_remove in drivers\bluetooth\btsdio.c in the Linux Kernel. In this flaw, a call to btsdio_remove with an unfinished job, may cause a race problem leading to a ...
Severity: High
Risk Score: 7.0
EPSS Percentile: 2.1%

CVE-2023-1476

Component: Linux
Version: 3.10.108
Description: A use-after-free flaw was found in the Linux kernel's mm/mremap memory address space accounting source code. This issue occurs due to a race condition between rmap walk and mremap, allowing a local us...
Severity: High
Risk Score: 7.0
EPSS Percentile: 2.8%

CVE-2023-1077

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, pick_next_rt_entity() may return a type confused entry, not detected by the BUG_ON condition, as the confused entry will not be NULL, but list_head.The buggy error condition would...
Severity: High
Risk Score: 7.0
EPSS Percentile: 3.2%

CVE-2022-48858

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix a race on command flush flow Fix a refcount use after free warning due to a race on command entry. Such race occurs ...
Severity: High
Risk Score: 7.0
EPSS Percentile: 20.6%

CVE-2022-48790

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: nvme: fix a possible use-after-free in controller reset during load Unlike .queue_rq, in .submit_async_event drivers may not check...
Severity: High
Risk Score: 7.0
EPSS Percentile: 10.5%

CVE-2022-45919

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 6.0.10. In drivers/media/dvb-core/dvb_ca_en50221.c, a use-after-free can occur is there is a disconnect after an open, because of the lack of a wait...
Severity: High
Risk Score: 7.0
EPSS Percentile: 1.7%

CVE-2022-45886

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 6.0.9. drivers/media/dvb-core/dvb_net.c has a .disconnect versus dvb_device_open race condition that leads to a use-after-free.
Severity: High
Risk Score: 7.0
EPSS Percentile: 1.3%

CVE-2022-45885

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 6.0.9. drivers/media/dvb-core/dvb_frontend.c has a race condition that can cause a use-after-free when a device is disconnected.

Severity: High
Risk Score: 7.0
EPSS Percentile: 1.1%

CVE-2022-45884

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 6.0.9. drivers/media/dvb-core/dvbdev.c has a use-after-free, related to dvb_register_device dynamically allocating fops.
Severity: High
Risk Score: 7.0
EPSS Percentile: 1.1%

CVE-2022-3649

Unreachable

Component: Linux
Version: 3.10.108
Description: A vulnerability was found in Linux Kernel. It has been classified as problematic. Affected is the function nilfs_new_inode of the file fs/nilfs2/inode.c of the component BPF. The manipulation leads to...
Severity: High
Risk Score: 7.0
EPSS Percentile: 24.1%

CVE-2022-3635 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: A vulnerability, which was classified as critical, has been found in Linux Kernel. Affected by this issue is the function tst_timer of the file drivers/atm/idt77252.c of the component IPsec. The manip...
Severity: High
Risk Score: 7.0
EPSS Percentile: 33.1%

CVE-2022-2961

Component: Linux
Version: 3.10.108
Description: A use-after-free flaw was found in the Linux kernel's PLP Rose functionality in the way a user triggers a race condition by calling bind while simultaneously triggering the rose_bind() function. This ...
Severity: High
Risk Score: 7.0
EPSS Percentile: 2.0%

CVE-2022-29582 🔥 PoC

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 5.17.3, fs/io_uring.c has a use-after-free due to a race condition in io_uring timeouts. This can be triggered by a local user who has no access to any user namespace; howev...
Severity: High
Risk Score: 7.0
EPSS Percentile: 27.3%

CVE-2022-2602 🔥 PoC

Component: Linux
Version: 3.10.108
Description: io_uring UAF, Unix SCM garbage collection
Severity: High
Risk Score: 7.0
EPSS Percentile: 74.0%

CVE-2022-1734 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: A flaw in Linux Kernel found in nfcmrvl_nci_unregister_dev() in drivers/nfc/nfcmrvl/main.c can lead to use after free both read or write when non synchronized between cleanup routine and firmware down...
Severity: High
Risk Score: 7.0
EPSS Percentile: 27.2%

CVE-2022-1048

Component: Linux
Version: 3.10.108
Description: A use-after-free flaw was found in the Linux kernel's sound subsystem in the way a user triggers concurrent calls of PCM hw_params. The hw_free ioctls or similar race condition happens inside ALSA PCM...
Severity: High
Risk Score: 7.0
EPSS Percentile: 0.7%

CVE-2021-47281

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: ALSA: seq: Fix race of snd_seq_timer_open() The timer instance per queue is exclusive, and snd_seq_timer_open() should have manage...
Severity: High
Risk Score: 7.0
EPSS Percentile: 2.2%

CVE-2021-47280

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: drm: Fix use-after-free read in drm_getunique() There is a time-of-check-to-time-of-use error in drm_getunique() due to retrieving...
Severity: High
Risk Score: 7.0
EPSS Percentile: 0.7%

CVE-2021-44733 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: A use-after-free exists in drivers/tee/tee_shm.c in the TEE subsystem in the Linux kernel through 5.15.11. This occurs because of a race condition in tee_shm_get_from_id during an attempt to free a sh...
Severity: High
Risk Score: 7.0
EPSS Percentile: 45.3%

CVE-2021-4202 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: A use-after-free flaw was found in nci_request in net/nfc/nci/core.c in NFC Controller Interface (NCI) in the Linux kernel. This flaw could allow a local attacker with user privileges to cause a data ...
Severity: High
Risk Score: 7.0
EPSS Percentile: 19.5%

CVE-2021-4083 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A read-after-free memory flaw was found in the Linux kernel's garbage collection for Unix domain socket file handlers in the way users call close() and fget() simultaneously and can potentially trigge...
Severity: High
Risk Score: 7.0
EPSS Percentile: 11.9%

CVE-2021-40490

Unreachable

Component: Linux
Version: 3.10.108
Description: A race condition was discovered in ext4_write_inline_data_end in fs/ext4/inline.c in the ext4 subsystem in the Linux kernel through 5.13.13.

Severity: High
Risk Score: 7.0
EPSS Percentile: 9.0%

CVE-2021-3640 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A flaw use-after-free in function sco_sock_sendmsg() of the Linux kernel HCI subsystem was found in the way user calls ioct UFFDIO_REGISTER or other way triggers race condition of the call sco_conn_de...
Severity: High
Risk Score: 7.0
EPSS Percentile: 5.1%

CVE-2021-3609 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: .A flaw was found in the CAN BCM networking protocol in the Linux kernel, where a local attacker can abuse a flaw in the CAN subsystem to corrupt memory, crash the system or escalate privileges. This ...
Severity: High
Risk Score: 7.0
EPSS Percentile: 17.3%

CVE-2021-3348

Unreachable

Component: Linux
Version: 3.10.108
Description: nbd_add_socket in drivers/block/nbd.c in the Linux kernel through 5.10.12 has an ndb_queue_rq use-after-free that could be triggered by local attackers (with access to the nbd device) via an I/O reque...
Severity: High
Risk Score: 7.0
EPSS Percentile: 27.4%

CVE-2021-32399 🔥 PoC

Component: Linux
Version: 3.10.108
Description: net/bluetooth/hci_request.c in the Linux kernel through 5.12.2 has a race condition for removal of the HCI controller.
Severity: High
Risk Score: 7.0
EPSS Percentile: 36.0%

CVE-2020-29370 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in kmem_cache_alloc_bulk in mm/slub.c in the Linux kernel before 5.5.11. The slowpath lacks the required TID increment, aka CID-fd4d9c7d0c71.
Severity: High
Risk Score: 7.0
EPSS Percentile: 61.3%

CVE-2020-25668 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A flaw was found in Linux Kernel because access to the global variable fg_console is not properly synchronized leading to a use after free in con_font_op.
Severity: High
Risk Score: 7.0
EPSS Percentile: 33.4%

CVE-2020-25212

Unreachable

Component: Linux
Version: 3.10.108
Description: A TOCTOU mismatch in the NFS client code in the Linux kernel before 5.8.3 could be used by local attackers to corrupt memory or possibly have unspecified other impact because a size check is in fs/nfs...
Severity: High
Risk Score: 7.0
EPSS Percentile: 7.3%

CVE-2019-13233 🔥 PoC

Component: Linux
Version: 3.10.108
Description: In arch/x86/lib/insn-eval.c in the Linux kernel before 5.1.9, there is a use-after-free for access to an LDT entry because of a race condition between modify_ldt() and a #BR exception for an MPX bound...
Severity: High
Risk Score: 7.0
EPSS Percentile: 52.8%

CVE-2019-12817

Component: Linux
Version: 3.10.108
Description: arch/powerpc/mm/mmu_context_book3s64.c in the Linux kernel before 5.1.15 for powerpc has a bug where unrelated processes may be able to read/write to one another's virtual memory under certain conditi...
Severity: High
Risk Score: 7.0
EPSS Percentile: 21.2%

CVE-2019-11599 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The coredump implementation in the Linux kernel before 5.0.10 does not use locking or other mechanisms to prevent vma layout or vma flags changes while it runs, which allows local users to obtain sens...
Severity: High
Risk Score: 7.0
EPSS Percentile: 67.1%

CVE-2019-11486

Component: Linux
Version: 3.10.108
Description: The Siemens R3964 line discipline driver in drivers/tty/n_r3964.c in the Linux kernel before 5.0.8 has multiple race conditions.
Severity: High
Risk Score: 7.0
EPSS Percentile: 14.8%

CVE-2018-5814

Component: Linux
Version: 3.10.108
Description: In the Linux Kernel before version 4.16.11, 4.14.43, 4.9.102, and 4.4.133, multiple race condition errors when handling probe, disconnect, and rebind operations can be exploited to trigger a use-after...
Severity: High
Risk Score: 7.0
EPSS Percentile: 6.4%

CVE-2018-14633

Component: Linux
Version: 3.10.108
Description: A security flaw was found in the chap_server_compute_md5() function in the ISCSI target code in the Linux kernel in a way an authentication request from an ISCSI initiator is processed. An unauthentic...
Severity: High
Risk Score: 7.0
EPSS Percentile: 92.9%

CVE-2017-18249

Unreachable

Component: Linux
Version: 3.10.108
Description: The add_free_nid function in fs/f2fs/node.c in the Linux kernel before 4.12 does not properly track an allocated nid, which allows local users to cause a denial of service (race condition) or possibly...
Severity: High
Risk Score: 7.0
EPSS Percentile: 22.7%

CVE-2017-10661 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: Race condition in fs/timerfd.c in the Linux kernel before 4.10.15 allows local users to gain privileges or cause a denial of service (list corruption or use-after-free) via simultaneous file-descripto...
Severity: High
Risk Score: 7.0
EPSS Percentile: 96.4%

CVE-2017-1000405 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The Linux Kernel versions 2.6.38 through 4.14 have a problematic use of pmd_mkdirty() in the touch_pmd() function inside the THP implementation. touch_pmd() can be reached by get_user_pages(). In such...
Severity: High
Risk Score: 7.0
EPSS Percentile: 86.0%

CVE-2017-0523

Component: Linux
Version: 3.10.108
Description: An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High ...
Severity: High
Risk Score: 7.0
EPSS Percentile: 17.5%

CVE-2016-6787 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: kernel/events/core.c in the performance subsystem in the Linux kernel before 4.0 mismanages locks during certain migrations, which allows local users to gain privileges via a crafted application, aka ...
Severity: High
Risk Score: 7.0
EPSS Percentile: 26.0%

CVE-2016-6786

Unreachable

Component: Linux
Version: 3.10.108
Description: kernel/events/core.c in the performance subsystem in the Linux kernel before 4.0 mismanages locks during certain migrations, which allows local users to gain privileges via a crafted application, aka ...
Severity: High
Risk Score: 7.0

EPSS Percentile: 26.0%

CVE-2016-2059

Component: Linux
Version: 3.10.108
Description: The msm_ipc_router_bind_control_port function in net/ipc_router/ipc_router_core.c in the IPC router kernel module for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contrib...
Severity: High
Risk Score: 7.0
EPSS Percentile: 9.0%

CVE-2016-10906

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in drivers/net/ethernet/arc/emac_main.c in the Linux kernel before 4.5. A use-after-free is caused by a race condition between the functions arc_emac_tx and arc_emac_tx_clean.
Severity: High
Risk Score: 7.0
EPSS Percentile: 21.2%

CVE-2016-10200

Component: Linux
Version: 3.10.108
Description: Race condition in the L2TPv3 IP Encapsulation feature in the Linux kernel before 4.8.14 allows local users to gain privileges or cause a denial of service (use-after-free) by making multiple bind syst...
Severity: High
Risk Score: 7.0
EPSS Percentile: 6.4%

CVE-2015-8963

Unreachable

Component: Linux
Version: 3.10.108
Description: Race condition in kernel/events/core.c in the Linux kernel before 4.4 allows local users to gain privileges or cause a denial of service (use-after-free) by leveraging incorrect handling of an swevent...
Severity: High
Risk Score: 7.0
EPSS Percentile: 27.0%

CVE-2015-0572

Component: Linux
Version: 3.10.108
Description: Multiple race conditions in drivers/char/adsprpc.c and drivers/char/adsprpc_compat.c in the ADSPRPC driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions ...

Severity: High
Risk Score: 7.0
EPSS Percentile: 19.5%

CVE-2014-9940

Unreachable

Component: Linux
Version: 3.10.108
Description: The regulator_ena_gpio_free function in drivers/regulator/core.c in the Linux kernel before 3.19 allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted appli...
Severity: High
Risk Score: 7.0
EPSS Percentile: 28.0%

CVE-2020-26541 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The Linux kernel through 5.8.13 does not properly enforce the Secure Boot Forbidden Signature Database (aka dbx) protection mechanism. This affects certs/blacklist.c and certs/system_keyring.c.
Severity: Medium
Risk Score: 6.9
EPSS Percentile: 22.8%

CVE-2013-4470 🔥 PoC

Reachable

Component: Linux
Version: 3.10.108
Description: The Linux kernel before 3.12, when UDP Fragmentation Offload (UFO) is enabled, does not properly initialize certain data structures, which allows local users to cause a denial of service (memory corru...
Severity: Medium
Risk Score: 6.9
EPSS Percentile: 45.4%

CVE-2023-2002 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: A vulnerability was found in the HCI sockets implementation due to a missing capability check in net/bluetooth/hci_sock.c in the Linux Kernel. This flaw allows an attacker to unauthorized execution of...
Severity: Medium
Risk Score: 6.8
EPSS Percentile: 57.3%

CVE-2021-4203 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: A use-after-free read flaw was found in sock_getsockopt() in net/core/sock.c due to SO_PEERCRED and SO_PEERGROUPS race with listen() (and connect()) in the Linux kernel. In this flaw, an attacker with...
Severity: Medium
Risk Score: 6.8
EPSS Percentile: 72.7%

CVE-2023-4273 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A flaw was found in the exFAT driver of the Linux kernel. The vulnerability exists in the implementation of the file name reconstruction function, which is responsible for reading file name entries fr...
Severity: Medium
Risk Score: 6.7
EPSS Percentile: 12.3%

CVE-2022-2503 🔥 PoC

Component: Linux
Version: 3.10.108
Description: Dm-verity is used for extending root-of-trust to root filesystems. LoadPin builds on this property to restrict module/firmware loads to just the trusted root filesystem. Device-mapper table reloads cu...
Severity: Medium
Risk Score: 6.7
EPSS Percentile: 42.3%

CVE-2021-43975 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel through 5.15.2, hw_atl_utils_fw_rpc_wait in drivers/net/ethernet/aquantia/atlantic/hw_atl/hw_atl_utils.c allows an attacker (who can introduce a crafted device) to trigger an out-o...
Severity: Medium
Risk Score: 6.7
EPSS Percentile: 35.1%

CVE-2021-42327 🔥 PoC

Component: Linux
Version: 3.10.108
Description: dp_link_settings_write in drivers/gpu/drm/amd/display/amdgpu_dm/amdgpu_dm_debugfs.c in the Linux kernel through 5.14.14 allows a heap-based buffer overflow by an attacker who can write a string to the...
Severity: Medium
Risk Score: 6.7

EPSS Percentile: 44.3%

CVE-2021-3411 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A flaw was found in the Linux kernel in versions prior to 5.10. A violation of memory access was found while detecting a padding of int3 in the linking state. The highest threat from this vulnerabilit...
Severity: Medium
Risk Score: 6.7
EPSS Percentile: 28.1%

CVE-2020-36694 🔥 PoC

Component: Linux
Version: 3.10.108
Description: An issue was discovered in netfilter in the Linux kernel before 5.10. There can be a use-after-free in the packet processing context, because the per-CPU sequence count is mishandled during concurrent...
Severity: Medium
Risk Score: 6.7
EPSS Percentile: 22.9%

CVE-2020-27777 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A flaw was found in the way RTAS handled memory accesses in userspace to kernel communication. On a locked down (usually due to Secure Boot) guest system running on top of PowerVM or KVM hypervisors (...
Severity: Medium
Risk Score: 6.7
EPSS Percentile: 19.5%

CVE-2020-15780 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in drivers/acpi/acpi_configfs.c in the Linux kernel before 5.7.7. Injection of malicious ACPI tables via configfs could be used by attackers to bypass lockdown and secure boot ...
Severity: Medium
Risk Score: 6.7
EPSS Percentile: 70.5%

CVE-2020-15436 🔥 PoC

Component: Linux
Version: 3.10.108
Description: Use-after-free vulnerability in fs/block_dev.c in the Linux kernel before 5.8 allows local users to gain privileges or cause a denial of service by leveraging improper access to a certain error field.
Severity: Medium

Risk Score: 6.7
EPSS Percentile: 31.1%

CVE-2020-12464 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: usb_sg_cancel in drivers/usb/core/message.c in the Linux kernel before 5.6.8 has a use-after-free because a transfer occurs without a reference, aka CID-056ad39ee925.
Severity: Medium
Risk Score: 6.7
EPSS Percentile: 70.3%

CVE-2022-1015 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A flaw was found in the Linux kernel in linux/net/netfilter/nf_tables_api.c of the netfilter subsystem. This flaw allows a local user to cause an out-of-bounds write issue.
Severity: Medium
Risk Score: 6.6
EPSS Percentile: 77.9%

CVE-2020-14331 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A flaw was found in the Linux kernel's implementation of the invert video code on VGA consoles when a local attacker attempts to resize the console, calling an ioctl VT_RESIZE, which causes an out-of-...
Severity: Medium
Risk Score: 6.6
EPSS Percentile: 5.2%

CVE-2023-3338 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A null pointer dereference flaw was found in the Linux kernel's DECnet networking protocol. This issue could allow a remote user to crash the system.
Severity: Medium
Risk Score: 6.5
EPSS Percentile: 93.3%

CVE-2020-29373 🔥 PoC

Component: Linux
Version: 3.10.108
Description: An issue was discovered in fs/io_uring.c in the Linux kernel before 5.6. It unsafely handles the root directory during path lookups, and thus a process inside a mount namespace can escape to unintende...
Severity: Medium

Risk Score: 6.5
EPSS Percentile: 24.4%

CVE-2019-5108 🔥 PoC

Component: Linux
Version: 3.10.108
Description: An exploitable denial-of-service vulnerability exists in the Linux kernel prior to mainline 5.3. An attacker could exploit this vulnerability by triggering AP to send IAPP location updates for station...
Severity: Medium
Risk Score: 6.5
EPSS Percentile: 70.6%

CVE-2019-3460 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A heap data infoleak in multiple locations including L2CAP_PARSE_CONF_RSP was found in the Linux kernel before 5.1-rc1.
Severity: Medium
Risk Score: 6.5
EPSS Percentile: 61.2%

CVE-2019-3459 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A heap address information leak while using L2CAP_GET_CONF_OPT was discovered in the Linux kernel before 5.1-rc1.
Severity: Medium
Risk Score: 6.5
EPSS Percentile: 70.8%

CVE-2022-45888 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 6.0.9. drivers/char/xillybus/xillyusb.c has a race condition and use-after-free during physical removal of a USB device.
Severity: Medium
Risk Score: 6.4
EPSS Percentile: 35.2%

CVE-2021-3573 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A use-after-free in function hci_sock_bound_ioctl() of the Linux kernel HCI subsystem was found in the way user calls ioct HCIUNBLOCKADDR or other way triggers race condition of the call hci_unregiste...
Severity: Medium

Risk Score: 6.4
EPSS Percentile: 5.4%

CVE-2021-0920 🔥 In VulnCheck KEV

Reachable

Component: Linux
Version: 3.10.108
Description: In unix_scm_to_skb of af_unix.c, there is a possible use after free bug due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interact...
Severity: Medium
Risk Score: 6.4
EPSS Percentile: 65.4%

CVE-2019-15214 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.0.10. There is a use-after-free in the sound subsystem because card disconnection causes certain data structures to be deleted too early. This is r...
Severity: Medium
Risk Score: 6.4
EPSS Percentile: 44.6%

CVE-2024-41012 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: filelock: Remove locks reliably when fcntl/close race is detected When fcntl_setlk() races with close(), it removes the created lo...
Severity: Medium
Risk Score: 6.3
EPSS Percentile: 10.3%

CVE-2023-40791 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: extract_user_to_sg in lib/scatterlist.c in the Linux kernel before 6.4.12 fails to unpin pages in a certain situation, as demonstrated by a WARNING for try_grab_page.
Severity: Medium
Risk Score: 6.3
EPSS Percentile: 16.2%

CVE-2014-5207 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: fs/namespace.c in the Linux kernel through 3.16.1 does not properly restrict clearing MNT_NODEV, MNT_NOSUID, and MNT_NOEXEC and changing MNT_ATIME_MASK during a remount of a bind mount, which allows l...
Severity: Medium
Risk Score: 6.2
EPSS Percentile: 45.7%

CVE-2014-5045 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The mountpoint_last function in fs/namei.c in the Linux kernel before 3.15.8 does not properly maintain a certain reference count during attempts to use the umount system call in conjunction with a sy...
Severity: Medium
Risk Score: 6.2
EPSS Percentile: 6.3%

CVE-2014-4014 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The capabilities implementation in the Linux kernel before 3.14.8 does not properly consider that namespaces are inapplicable to inodes, which allows local users to bypass intended chmod restrictions ...
Severity: Medium
Risk Score: 6.2
EPSS Percentile: 82.1%

CVE-2013-6368 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The KVM subsystem in the Linux kernel through 3.12.5 allows local users to gain privileges or cause a denial of service (system crash) via a VAPIC synchronization operation involving a page-end addres...
Severity: Medium
Risk Score: 6.2
EPSS Percentile: 22.9%

CVE-2019-19602 🔥 PoC

Component: Linux
Version: 3.10.108
Description: fpregs_state_valid in arch/x86/include/asm/fpu/internal.h in the Linux kernel before 5.4.2, when GCC 9 is used, allows context-dependent attackers to cause a denial of service (memory corruption) or p...
Severity: Medium
Risk Score: 6.1
EPSS Percentile: 52.3%

CVE-2014-2309 🔥 PoC

Reachable

Component: Linux
Version: 3.10.108
Description: The ip6_route_add function in net/ipv6/route.c in the Linux kernel through 3.13.6 does not properly count the addition of routes, which allows remote attackers to cause a denial of service (memory con...
Severity: Medium
Risk Score: 6.1
EPSS Percentile: 86.4%

CVE-2013-7027 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The ieee80211_radiotap_iterator_init function in net/wireless/radiotap.c in the Linux kernel before 3.11.7 does not check whether a frame contains any data outside of the header, which might allow att...
Severity: Medium
Risk Score: 6.1
EPSS Percentile: 76.8%

CVE-2013-4387 🔥 PoC

Reachable

Component: Linux
Version: 3.10.108
Description: net/ipv6/ip6_output.c in the Linux kernel through 3.11.4 does not properly determine the need for UDP Fragmentation Offload (UFO) processing of small packets after the UFO queueing of a large packet, ...
Severity: Medium
Risk Score: 6.1
EPSS Percentile: 90.8%

CVE-2020-25211 🔥 PoC

Reachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel through 5.8.7, local attackers able to inject conntrack netlink configuration could overflow a local buffer, causing crashes or triggering use of incorrect protocol numbers in ctne...
Severity: Medium
Risk Score: 6.0
EPSS Percentile: 6.9%

CVE-2013-4299 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108

Description: Interpretation conflict in drivers/md/dm-snap-persistent.c in the Linux kernel through 3.11.6 allows remote authenticated users to obtain sensitive information or modify data via a crafted mapping to ...
Severity: Medium
Risk Score: 6.0
EPSS Percentile: 74.0%

CVE-2020-8649 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the vgacon_invert_region function in drivers/video/console/vgacon.c.
Severity: Medium
Risk Score: 5.9
EPSS Percentile: 45.1%

CVE-2020-28097 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The vgacon subsystem in the Linux kernel before 5.8.10 mishandles software scrollback. There is a vgacon_scrolldelta out-of-bounds read, aka CID-973c096f6a85.
Severity: Medium
Risk Score: 5.9
EPSS Percentile: 36.0%

CVE-2018-1108 🔥 PoC

Component: Linux
Version: 3.10.108
Description: kernel drivers before version 4.17-rc1 are vulnerable to a weakness in the Linux kernel's implementation of random seed data. Programs, early in the boot sequence, could use the data allocated for the...
Severity: Medium
Risk Score: 5.9
EPSS Percentile: 76.0%

CVE-2013-6367 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The apic_get_tmcct function in arch/x86/kvm/lapic.c in the KVM subsystem in the Linux kernel through 3.12.5 allows guest OS users to cause a denial of service (divide-by-zero error and host OS crash) ...
Severity: Medium
Risk Score: 5.7
EPSS Percentile: 71.2%

CVE-2023-1998 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The Linux kernel allows userspace processes to enable mitigations by calling prctl with PR_SET_SPECULATION_CTRL which disables the speculation feature as well as by using seccomp. We had noticed that ...
Severity: Medium
Risk Score: 5.6
EPSS Percentile: 41.8%

CVE-2019-7308 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: kernel/bpf/verifier.c in the Linux kernel before 4.20.6 performs undesirable out-of-bounds speculation on pointer arithmetic in various cases, including cases of different branches with different stat...
Severity: Medium
Risk Score: 5.6
EPSS Percentile: 26.4%

CVE-2024-47674 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: mm: avoid leaving partial pfn mappings around in error case As Jann points out, PFN mappings are special, because unlike normal me...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 8.5%

CVE-2024-44947 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: fuse: Initialize beyond-EOF page contents before setting uptodate fuse_notify_store(), unlike fuse_do_readpage(), does not enable ...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 77.0%

CVE-2024-25741 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: printer_write in drivers/usb/gadget/function/f_printer.c in the Linux kernel through 6.7.4 does not properly call usb_ep_queue, which might allow attackers to cause a denial of service or have unspeci...

Severity: Medium
Risk Score: 5.5
EPSS Percentile: 11.5%

CVE-2023-6560 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An out-of-bounds memory access flaw was found in the io_uring SQ/CQ rings functionality in the Linux kernel. This issue could allow a local user to crash the system.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 5.1%

CVE-2023-52587 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: IB/ipoib: Fix mcast list locking Releasing the `priv->lock` while iterating the `priv->multicast_list` in `ipoib_mcast_join_task()...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 0.3%

CVE-2023-4569 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: A memory leak flaw was found in nft_set_catchall_flush in net/netfilter/nf_tables_api.c in the Linux Kernel. This issue may allow a local attacker to cause double-deactivations of catchall elements, w...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 0.4%

CVE-2023-42755 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A flaw was found in the IPv4 Resource Reservation Protocol (RSVP) classifier in the Linux kernel. The xprt pointer may go beyond the linear part of the skb, leading to an out-of-bounds read in the `rs...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 30.9%

CVE-2023-42754 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A NULL pointer dereference flaw was found in the Linux kernel ipv4 stack. The socket buffer (skb) was assumed to be associated with a device before calling __ip_options_compile, which is not always th...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 5.1%

CVE-2023-37454 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 6.4.2. A crafted UDF filesystem image causes a use-after-free write operation in the udf_put_super and udf_close_lvid functions in fs/udf/super.c. N...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 30.2%

CVE-2023-1249 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A use-after-free flaw was found in the Linux kernel's core dump subsystem. This flaw allows a local user to crash the system. Only if patch 390031c94211 ("coredump: Use the vma snapshot in fill_files_...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 10.4%

CVE-2023-0469 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: A use-after-free flaw was found in io_uring/filetable.c in io_install_fixed_file in the io_uring subcomponent in the Linux Kernel during call cleanup. This flaw may lead to a denial of service.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 15.1%

CVE-2023-0160 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A deadlock flaw was found in the Linux kernel's BPF subsystem. This flaw allows a local user to potentially crash the system.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 5.1%

CVE-2022-47929 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 6.1.6, a NULL pointer dereference bug in the traffic control subsystem allows an unprivileged user to trigger a denial of service (system crash) via a crafted traffic contro...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 30.1%

CVE-2022-45869 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A race condition in the x86 KVM subsystem in the Linux kernel through 6.1-rc6 allows guest OS users to cause a denial of service (host OS crash or host OS memory corruption) when nested virtualisation...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 15.1%

CVE-2022-4543 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A flaw named "EntryBleed" was found in the Linux Kernel Page Table Isolation (KPTI). This issue could allow a local attacker to leak KASLR base via prefetch side-channels based on TLB timing for Intel...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 32.8%

CVE-2022-42703 🔥 PoC

Component: Linux
Version: 3.10.108
Description: mm/rmap.c in the Linux kernel before 5.19.7 has a use-after-free related to leaf anon_vma double reuse.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 68.1%

CVE-2022-41218 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In drivers/media/dvb-core/dmxdev.c in the Linux kernel through 5.19.10, there is a use-after-free caused by refcount races, affecting dvb_demux_open and dvb_dmxdev_release.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 55.8%

CVE-2022-2905 PoC

Component: Linux
Version: 3.10.108
Description: An out-of-bounds memory read flaw was found in the Linux kernel's BPF subsystem in how a user calls the bpf_tail_call function with a key larger than the max_entries of the map. This flaw allows a loc...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 5.1%

CVE-2022-28356 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 5.17.1, a refcount leak bug was found in net/llc/af_llc.c.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 30.1%

CVE-2022-2153 PoC

Component: Linux
Version: 3.10.108
Description: A flaw was found in the Linux kernel's KVM when attempting to set a SynIC IRQ. This issue makes it possible for a misbehaving VMM to write to SYNIC/STIMER MSRs, causing a NULL pointer dereference. Thi...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 5.2%

CVE-2022-2078 PoC

Component: Linux
Version: 3.10.108
Description: A vulnerability was found in the Linux kernel's nft_set_desc_concat_parse() function .This flaw allows an attacker to trigger a buffer overflow via nft_set_desc_concat_parse() , causing a denial of se...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 59.9%

CVE-2022-1263 PoC

Component: Linux
Version: 3.10.108
Description: A NULL pointer dereference issue was found in KVM when releasing a vCPU with dirty ring support enabled. This flaw allows an unprivileged local attacker on the host to issue specific ioctl calls, caus...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 15.2%

CVE-2022-1204 PoC

Component: Linux
Version: 3.10.108
Description: A use-after-free flaw was found in the Linux kernel's Amateur Radio AX.25 protocol functionality in the way a user connects with the protocol. This flaw allows a local user to crash the system.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 5.1%

CVE-2022-1198 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: A use-after-free vulnerabilitity was discovered in drivers/net/hamradio/6pack.c of linux that allows an attacker to crash linux kernel by simulating ax25 device using 6pack driver from user space.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 27.3%

CVE-2022-1016 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: A flaw was found in the Linux kernel in net/netfilter/nf_tables_core.c:nft_do_chain, which can cause a use-after-free. This issue needs to handle 'return' with proper preconditions, as it can lead to ...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 20.5%

CVE-2022-0854 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A memory leak flaw was found in the Linux kernel's DMA subsystem, in the way a user calls DMA_FROM_DEVICE. This flaw allows a local user to read random memory from the kernel space.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 5.1%

CVE-2022-0382 🔥 PoC

Component: Linux
Version: 3.10.108
Description: An information leak flaw was found due to uninitialized memory in the Linux kernel's TIPC protocol subsystem, in the way a user sends a TIPC datagram to one or more destinations. This flaw allows a lo...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 12.0%

CVE-2021-45868 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 5.15.3, fs/quota/quota_tree.c does not validate the block number in the quota tree (on disk). This can, for example, lead to a kernel/locking/rwsem.c use-after-free if there...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 47.3%

CVE-2021-45402 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The check_alu_op() function in kernel/bpf/verifier.c in the Linux kernel through v5.16-rc5 did not properly update bounds while handling the mov32 instruction, which allows local users to obtain poten...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 19.5%

CVE-2021-44879 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In gc_data_segment in fs/f2fs/gc.c in the Linux kernel before 5.16.3, special files are not considered, leading to a move_data_page NULL pointer dereference.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 45.7%

CVE-2021-4442 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel, the following vulnerability has been resolved: tcp: add sanity tests to TCP_QUEUE_SEQ Qingyu Li reported a syzkaller bug where the repro changes RCV SEQ _after_ restoring data i...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 19.5%

CVE-2021-43389 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108

Description: An issue was discovered in the Linux kernel before 5.14.15. There is an array-index-out-of-bounds flaw in the detach_capi_ctr function in drivers/isdn/capi/kcapi.c.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 35.9%

CVE-2021-4150 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: A use-after-free flaw was found in the add_partition in block/partitions/core.c in the Linux kernel. A local attacker with user privileges could cause a denial of service on the system. The issue resu...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 19.5%

CVE-2021-4149 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: A vulnerability was found in btrfs_alloc_tree_b in fs/btrfs/extent-tree.c in the Linux kernel due to an improper lock operation in btrfs. In this flaw, a user with a local privilege may cause a denial...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 27.3%

CVE-2021-4148 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: A vulnerability was found in the Linux kernel's block_invalidatepage in fs/buffer.c in the filesystem. A missing sanity check may allow a local attacker with user privilege to cause a denial of servic...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 19.5%

CVE-2021-4095 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A NULL pointer dereference was found in the Linux kernel's KVM when dirty ring logging is enabled without an active vCPU context. An unprivileged local attacker on the host may use this flaw to cause ...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 29.2%

CVE-2021-38208 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: net/nfc/llcp_sock.c in the Linux kernel before 5.12.10 allows local unprivileged users to cause a denial of service (NULL pointer dereference and BUG) by making a getsockname call after a certain type...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 30.1%

CVE-2021-38203 🔥 PoC

Component: Linux
Version: 3.10.108
Description: btrfs in the Linux kernel before 5.13.4 allows attackers to cause a denial of service (deadlock) via processes that trigger allocation of new system chunks during times when there is a shortage of fre...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 25.8%

CVE-2021-38198 🔥 PoC

Component: Linux
Version: 3.10.108
Description: arch/x86/kvm/mmu/paging_tmpl.h in the Linux kernel before 5.12.11 incorrectly computes the access permissions of a shadow page, leading to a missing guest protection page fault.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 27.8%

CVE-2021-3744 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: A memory leak flaw was found in the Linux kernel in the ccp_run_aes_gcm_cmd() function in drivers/crypto/ccp/ccp-ops.c, which allows attackers to cause a denial of service (memory consumption). This v...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 37.6%

CVE-2021-34693 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: net/can/bcm.c in the Linux kernel through 5.12.10 allows local users to obtain sensitive information from kernel stack memory because parts of a data structure are uninitialized.
Severity: Medium
Risk Score: 5.5

EPSS Percentile: 14.7%

CVE-2020-27194 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.8.15. scalar32_min_max_or in kernel/bpf/verifier.c mishandles bounds tracking during use of 64-bit values, aka CID-5b9fbeb75b6a.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 89.8%

CVE-2020-27152 🔥 PoC

Component: Linux
Version: 3.10.108
Description: An issue was discovered in ioapic_lazy_update_eoi in arch/x86/kvm/ioapic.c in the Linux kernel before 5.9.2. It has an infinite loop related to improper interaction between a resampler and edge trigge...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 27.8%

CVE-2020-25673 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A vulnerability was found in Linux kernel where non-blocking socket in llcp_sock_connect() leads to leak and eventually hanging-up the system.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 32.6%

CVE-2020-12771 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 5.6.11. btree_gc_coalesce in drivers/md/bcache/btree.c has a deadlock if a coalescing operation fails.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 45.4%

CVE-2020-12769 🔥 PoC

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.4.17. drivers/spi/spi-dw.c allows attackers to cause a panic via concurrent calls to dw_spi_irq and dw_spi_transfer_one, aka CID-19b61392c5a8.

Severity: Medium
Risk Score: 5.5
EPSS Percentile: 19.8%

CVE-2019-7222 PoC

Component: Linux
Version: 3.10.108
Description: The KVM implementation in the Linux kernel through 4.20.5 has an Information Leak.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 43.5%

CVE-2019-19922 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: kernel/sched/fair.c in the Linux kernel before 5.3.9, when cpu.cfs_quota_us is used (e.g., with Kubernetes), allows attackers to cause a denial of service against non-cpu-bound applications by generat...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 61.0%

CVE-2019-19767 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The Linux kernel before 5.4.2 mishandles ext4_expand_extra_isize, as demonstrated by use-after-free errors in __ext4_expand_extra_isize and ext4_xattr_set_entry, related to fs/ext4/inode.c and fs/ext4...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 74.9%

CVE-2019-19037 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: ext4_empty_dir in fs/ext4/namei.c in the Linux kernel through 5.3.12 allows a NULL pointer dereference because ext4_read_dirblock(inode,0,DIRENT_HTREE) can be zero.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 76.8%

CVE-2019-19036 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: btrfs_root_node in fs/btrfs/ctree.c in the Linux kernel through 5.3.12 allows a NULL pointer dereference because rcu_dereference(root->node) can be zero.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 77.5%

CVE-2019-18885 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: fs/btrfs/volumes.c in the Linux kernel before 5.1 allows a btrfs_verify_dev_extents NULL pointer dereference via a crafted btrfs image because fs_devices->devices is mishandled within find_device, aka...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 84.7%

CVE-2019-15924 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.0.11. fm10k_init_module in drivers/net/ethernet/intel/fm10k/fm10k_main.c has a NULL pointer dereference because there is no -ENOMEM upon an alloc_w...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 40.3%

CVE-2019-15923 🔥 PoC

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.0.9. There is a NULL pointer dereference for a cd data structure if alloc_disk fails in drivers/block/paride/pf.c.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 36.1%

CVE-2019-15922 🔥 PoC

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.0.9. There is a NULL pointer dereference for a pf data structure if alloc_disk fails in drivers/block/paride/pf.c.
Severity: Medium
Risk Score: 5.5

EPSS Percentile: 36.1%

CVE-2018-7755 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the fd_locked_ioctl function in drivers/block/floppy.c in the Linux kernel through 4.15.7. The floppy driver will copy a kernel pointer to user memory in response to the FDG...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 34.4%

CVE-2018-7740 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The resv_map_release function in mm/hugetlb.c in the Linux kernel through 4.15.7 allows local users to cause a denial of service (BUG) via a crafted application that makes mmap system calls and has a ...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 25.3%

CVE-2018-7492 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: A NULL pointer dereference was found in the net/rds/rdma.c __rds_rdma_map() function in the Linux kernel before 4.14.7 allowing local attackers to cause a system panic and a denial-of-service, related...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 24.6%

CVE-2018-7273 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel through 4.15.4, the floppy driver reveals the addresses of kernel functions and global variables using printk calls within the function show_floppy in drivers/block/floppy.c. An at...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 81.4%

CVE-2018-7191 🔥 PoC

Component: Linux
Version: 3.10.108
Description: In the tun subsystem in the Linux kernel before 4.13.14, dev_get_valid_name is not called before register_netdevice. This allows local users to cause a denial of service (NULL pointer dereference and ...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 26.2%

CVE-2018-5803 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux Kernel before version 4.15.8, 4.14.25, 4.9.87, 4.4.121, 4.1.51, and 3.2.102, an error in the "_sctp_make_chunk()" function (net/sctp/sm_make_chunk.c) when handling SCTP packets length can...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 30.6%

CVE-2018-5333 🔥 Weaponized

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel through 4.14.13, the rds_cmsg_atomic function in net/rds/rdma.c mishandles cases where page pinning fails or an invalid address is supplied, leading to an rds_atomic_free_op NULL p...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 81.8%

CVE-2018-18690 🔥 PoC

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 4.17, a local attacker able to set attributes on an xfs filesystem could make this filesystem non-operational until the next mount by triggering an unchecked error condition...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 25.8%

CVE-2018-18397 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The userfaultfd implementation in the Linux kernel before 4.19.7 mishandles access control for certain UFFDIO_ ioctl calls, as demonstrated by allowing local users to write data into holes in a tmpfs ...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 21.9%

CVE-2018-14656 🔥 Commercial Exploit

Component: Linux
Version: 3.10.108
Description: A missing address check in the callers of the show_opcodes() in the Linux kernel allows an attacker to dump the kernel memory at an arbitrary kernel address into the dmesg log.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 27.7%

CVE-2018-14617 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 4.17.10. There is a NULL pointer dereference and panic in hfsplus_lookup() in fs/hfsplus/dir.c when opening a file (that is purportedly a hard link)...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 49.1%

CVE-2018-14616 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 4.17.10. There is a NULL pointer dereference in fscrypt_do_page_crypto() in fs/crypto/crypto.c when operating on a file in a corrupted f2fs image.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 50.4%

CVE-2018-14615 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 4.17.10. There is a buffer overflow in truncate_inline_inode() in fs/f2fs/inline.c when umounting an f2fs image, because a length value may be negat...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 51.9%

CVE-2018-14613 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108

Description: An issue was discovered in the Linux kernel through 4.17.10. There is an invalid pointer dereference in io_ctl_map_page() when mounting and operating a crafted btrfs image, because of a lack of block ...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 45.6%

CVE-2018-14612 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 4.17.10. There is an invalid pointer dereference in btrfs_root_node() when mounting a crafted btrfs image, because of a lack of chunk block group ma...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 45.6%

CVE-2018-14611 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 4.17.10. There is a use-after-free in try_merge_free_space() when mounting a crafted btrfs image, because of a lack of chunk type flag checks in btr...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 49.1%

CVE-2018-14610 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 4.17.10. There is out-of-bounds access in write_extent_buffer() when mounting and operating a crafted btrfs image, because of a lack of verification...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 45.4%

CVE-2018-14609 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 4.17.10. There is an invalid pointer dereference in __del_reloc_root() in fs/btrfs/relocation.c when mounting a crafted btrfs image, related to remo...

Severity: Medium
Risk Score: 5.5
EPSS Percentile: 50.4%

CVE-2018-13099 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in fs/f2fs/inline.c in the Linux kernel through 4.4. A denial of service (out-of-bounds memory access and BUG) can occur for a modified f2fs filesystem image in which an inline...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 72.4%

CVE-2018-13094 🔥 PoC

Component: Linux
Version: 3.10.108
Description: An issue was discovered in fs/xfs/libxfs/xfs_attr_leaf.c in the Linux kernel through 4.17.3. An OOPS may occur for a corrupted xfs image after xfs_da_shrink_inode() is called with a NULL bp.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 68.8%

CVE-2018-12896 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 4.17.3. An Integer Overflow in kernel/time/posix-timers.c in the POSIX timer code is caused by the way the overrun accounting works. Depending on in...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 21.7%

CVE-2018-11508 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The compat_get_timex function in kernel/compat.c in the Linux kernel before 4.16.9 allows local users to obtain sensitive information from kernel memory via adjtimex.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 80.5%

CVE-2018-1095 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The ext4_xattr_check_entries function in fs/ext4/xattr.c in the Linux kernel through 4.15.15 does not properly validate xattr sizes, which causes misinterpretation of a size as an error code, and cons...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 45.9%

CVE-2018-1094 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The ext4_fill_super function in fs/ext4/super.c in the Linux kernel through 4.15.15 does not always initialize the crc32c checksum driver, which allows attackers to cause a denial of service (ext4_xat...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 54.0%

CVE-2018-10881 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bound access in ext4_get_group_info function, a denial of service, and a system crash by mounting and operating...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 23.4%

CVE-2018-10880 🔥 PoC

Component: Linux
Version: 3.10.108
Description: Linux kernel is vulnerable to a stack-out-of-bounds write in the ext4 filesystem code when mounting and writing to a crafted ext4 image in ext4_update_inline_data(). An attacker could use this to caus...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 80.5%

CVE-2018-10323 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The xfs_bmap_extents_to_btree function in fs/xfs/libxfs/xfs_bmap.c in the Linux kernel through 4.16.3 allows local users to cause a denial of service (xfs_bmapi_write NULL pointer dereference) via a c...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 25.4%

CVE-2018-10322 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The xfs_dinode_verify function in fs/xfs/libxfs/xfs_inode_buf.c in the Linux kernel through 4.16.3 allows local users to cause a denial of service (xfs_ilock_attr_map_shared invalid pointer dereferenc...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 15.9%

CVE-2018-10124 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The kill_something_info function in kernel/signal.c in the Linux kernel before 4.13, when an unspecified architecture and compiler is used, might allow local users to cause a denial of service via an ...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 23.7%

CVE-2017-9150 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The do_check function in kernel/bpf/verifier.c in the Linux kernel before 4.11.1 does not make the allow_ptr_leaks value available for restricting the output of the print_bpf_insn function, which allo...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 66.5%

CVE-2017-7472 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The KEYS subsystem in the Linux kernel before 4.10.13 allows local users to cause a denial of service (memory consumption) via a series of KEY_REQKEY_DEFL_THREAD_KEYRING keyctl_set_reqkey_keyring call...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 70.5%

CVE-2017-2671 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The ping_unhash function in net/ipv4/ping.c in the Linux kernel through 4.10.8 is too late in obtaining a certain lock and consequently cannot ensure that disconnect function calls are safe, which all...
Severity: Medium

Risk Score: 5.5
EPSS Percentile: 61.1%

CVE-2017-18344 🔥 Commercial Exploit

Unreachable

Component: Linux
Version: 3.10.108
Description: The timer_create syscall implementation in kernel/time/posix-timers.c in the Linux kernel before 4.14.8 doesn't properly validate the sigevent->sigev_notify field, which leads to out-of-bounds access ...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 91.9%

CVE-2017-16994 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The walk_hugetlb_range function in mm/pagewalk.c in the Linux kernel before 4.14.2 mishandles holes in hugetlb ranges, which allows local users to obtain sensitive information from uninitialized kerne...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 89.0%

CVE-2017-14489 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The iscsi_if_rx function in drivers/scsi/scsi_transport_iscsi.c in the Linux kernel through 4.13.2 allows local users to cause a denial of service (panic) by leveraging incorrect length validation.
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 50.5%

CVE-2016-6828 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The tcp_check_send_head function in include/net/tcp.h in the Linux kernel before 4.7.5 does not properly maintain certain SACK state after a failed data copy, which allows local users to cause a denia...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 30.6%

CVE-2016-6198 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The filesystem layer in the Linux kernel before 4.5.5 proceeds with post-rename operations after an OverlayFS file is renamed to a self-hardlink, which allows local users to cause a denial of service ...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 12.2%

CVE-2016-4578 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: sound/core/timer.c in the Linux kernel through 4.6 does not initialize certain r1 data structures, which allows local users to obtain sensitive information from kernel stack memory via crafted use of ...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 50.4%

CVE-2015-8953 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: fs/overlayfs/copy_up.c in the Linux kernel before 4.2.6 uses an incorrect cleanup code path, which allows local users to cause a denial of service (dentry reference leak) via filesystem operations on ...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 22.4%

CVE-2015-1350 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The VFS subsystem in the Linux kernel 3.x provides an incomplete set of requirements for setattr operations that underspecifies removing extended privilege attributes, which allows local users to caus...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 7.8%

CVE-2014-8559 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The d_walk function in fs/dcache.c in the Linux kernel through 3.17.2 does not properly maintain the semantics of rename_lock, which allows local users to cause a denial of service (deadlock and syste...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 43.5%

CVE-2014-7970 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The pivot_root implementation in fs/namespace.c in the Linux kernel through 3.17 does not properly interact with certain locations of a chroot directory, which allows local users to cause a denial of ...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 18.5%

CVE-2014-3610 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The WRMSR processing functionality in the KVM subsystem in the Linux kernel through 3.17.2 does not properly handle the writing of a non-canonical address to a model-specific register, which allows gu...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 36.0%

CVE-2014-0155 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The ioapic_deliver function in virt/kvm/ioapic.c in the Linux kernel through 3.14.1 does not properly validate the kvm_irq_delivery_to_apic return value, which allows guest OS users to cause a denial ...
Severity: Medium
Risk Score: 5.5
EPSS Percentile: 45.2%

CVE-2020-12826 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A signal access-control issue was discovered in the Linux kernel before 5.6.5, aka CID-7395ea4e65c2. Because exec_id in include/linux/sched.h is only 32 bits, an integer overflow can interfere with a ...
Severity: Medium
Risk Score: 5.3
EPSS Percentile: 26.5%

CVE-2020-10942 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 5.5.8, get_raw_socket in drivers/vhost/net.c lacks validation of an sk_family field, which might allow attackers to trigger kernel stack corruption via crafted system calls.
Severity: Medium

Risk Score: 5.3
EPSS Percentile: 29.3%

CVE-2018-1120 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A flaw was found affecting the Linux kernel before version 4.17. By mmap()ing a FUSE-backed file onto a process's memory containing command line arguments (or environment strings), an attacker can cau...
Severity: Medium
Risk Score: 5.3
EPSS Percentile: 75.9%

CVE-2013-7446 🔥 PoC

Reachable

Component: Linux
Version: 3.10.108
Description: Use-after-free vulnerability in net/unix/af_unix.c in the Linux kernel before 4.3.3 allows local users to bypass intended AF_UNIX socket permissions or cause a denial of service (panic) via crafted ep...
Severity: Medium
Risk Score: 5.3
EPSS Percentile: 19.3%

CVE-2013-6376 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The recalculate_apic_map function in arch/x86/kvm/lapic.c in the KVM subsystem in the Linux kernel through 3.12.5 allows guest OS users to cause a denial of service (host OS crash) via a crafted ICR w...
Severity: Medium
Risk Score: 5.2
EPSS Percentile: 64.9%

CVE-2020-36558 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A race condition in the Linux kernel before 5.5.7 involving VT_RESIZEX could lead to a NULL pointer dereference and general protection fault.
Severity: Medium
Risk Score: 5.1
EPSS Percentile: 26.5%

CVE-2020-28974 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: A slab-out-of-bounds read in fbcon in the Linux kernel before 5.9.7 could be used by local attackers

to read privileged information or potentially crash the kernel, aka CID-3c4e0dff2095. This occurs b...
Severity: Medium
Risk Score: 5.0
EPSS Percentile: 18.3%

CVE-2015-1593 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The stack randomization feature in the Linux kernel before 3.19.1 on 64-bit platforms uses incorrect data types for the results of bitwise left-shift operations, which makes it easier for attackers to...
Severity: Medium
Risk Score: 5.0
EPSS Percentile: 82.4%

CVE-2014-7841 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The sctp_process_param function in net/sctp/sm_make_chunk.c in the SCTP implementation in the Linux kernel before 3.17.4, when ASCONF is used, allows remote attackers to cause a denial of service (NUL...
Severity: Medium
Risk Score: 5.0
EPSS Percentile: 97.9%

CVE-2014-3688 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The SCTP implementation in the Linux kernel before 3.17.4 allows remote attackers to cause a denial of service (memory consumption) by triggering a large number of chunks in an association's output qu...
Severity: Medium
Risk Score: 5.0
EPSS Percentile: 96.4%

CVE-2013-4350 PoC

Component: Linux
Version: 3.10.108
Description: The IPv6 SCTP implementation in net/sctp/ipv6.c in the Linux kernel through 3.11.1 uses data structures and function calls that do not trigger an intended configuration of IPsec encryption, which allo...
Severity: Medium
Risk Score: 5.0
EPSS Percentile: 73.2%

CVE-2018-12904 PoC

Component: Linux
Version: 3.10.108
Description: In arch/x86/kvm/vmx.c in the Linux kernel before 4.17.2, when nested virtualization is used, local attackers could cause L1 KVM guests to VMEXIT, potentially allowing privilege escalations and denial ...
Severity: Medium
Risk Score: 4.9
EPSS Percentile: 41.6%

CVE-2015-7799 🔥 PoC

Reachable

Component: Linux
Version: 3.10.108
Description: The slhc_init function in drivers/net/slip/slhc.c in the Linux kernel through 4.2.3 does not ensure that certain slot numbers are valid, which allows local users to cause a denial of service (NULL poi...
Severity: Medium
Risk Score: 4.9
EPSS Percentile: 29.2%

CVE-2015-3636 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The ping_unhash function in net/ipv4/ping.c in the Linux kernel before 4.0.3 does not initialize a certain list data structure during an unhash operation, which allows local users to gain privileges o...
Severity: Medium
Risk Score: 4.9
EPSS Percentile: 84.9%

CVE-2014-8481 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The instruction decoder in arch/x86/kvm/emulate.c in the KVM subsystem in the Linux kernel before 3.18-rc2 does not properly handle invalid instructions, which allows guest OS users to cause a denial ...
Severity: Medium
Risk Score: 4.9
EPSS Percentile: 49.5%

CVE-2014-8480 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The instruction decoder in arch/x86/kvm/emulate.c in the KVM subsystem in the Linux kernel before 3.18-rc2 lacks intended decoder-table flags for certain RIP-relative instructions, which allows guest ...
Severity: Medium
Risk Score: 4.9
EPSS Percentile: 49.5%

CVE-2014-7283 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The xfs_da3_fixhashpath function in fs/xfs/xfs_da_btree.c in the xfs implementation in the Linux kernel before 3.14.2 does not properly compare btree hash values, which allows local users to cause a d...
Severity: Medium
Risk Score: 4.9
EPSS Percentile: 19.5%

CVE-2014-3145 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The BPF_S_ANC_NLATTR_NEST extension implementation in the sk_run_filter function in net/core/filter.c in the Linux kernel through 3.14.3 uses the reverse order in a certain subtraction, which allows l...
Severity: Medium
Risk Score: 4.9
EPSS Percentile: 55.9%

CVE-2014-3144 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The (1) BPF_S_ANC_NLATTR and (2) BPF_S_ANC_NLATTR_NEST extension implementations in the sk_run_filter function in net/core/filter.c in the Linux kernel through 3.14.3 do not check whether a certain le...
Severity: Medium
Risk Score: 4.9
EPSS Percentile: 55.9%

CVE-2013-4516 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The mp_get_count function in drivers/staging/sb105x/sb_pci_mp.c in the Linux kernel before 3.12 does not initialize a certain data structure, which allows local users to obtain sensitive information f...
Severity: Medium
Risk Score: 4.9
EPSS Percentile: 10.8%

CVE-2016-5696 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: net/ipv4/tcp_input.c in the Linux kernel before 4.7 does not properly determine the rate of challenge ACK segments, which makes it easier for remote attackers to hijack TCP sessions via a blind in-win...
Severity: Medium

Risk Score: 4.8
EPSS Percentile: 96.7%

CVE-2023-42756 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A flaw was found in the Netfilter subsystem of the Linux kernel. A race condition between IPSET_CMD_ADD and IPSET_CMD_SWAP can lead to a kernel panic due to the invocation of `__ip_set_put` on a wrong...
Severity: Medium
Risk Score: 4.7
EPSS Percentile: 19.5%

CVE-2023-0468 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: A use-after-free flaw was found in io_uring/poll.c in io_poll_check_events in the io_uring subcomponent in the Linux Kernel due to a race condition of poll_refs. This flaw may cause a NULL pointer der...
Severity: Medium
Risk Score: 4.7
EPSS Percentile: 15.1%

CVE-2022-3303 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A race condition flaw was found in the Linux kernel sound subsystem due to improper locking. It could lead to a NULL pointer dereference while handling the SNDCTL_DSP_SYNC ioctl. A privileged local us...
Severity: Medium
Risk Score: 4.7
EPSS Percentile: 5.1%

CVE-2022-1205 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A NULL pointer dereference flaw was found in the Linux kernel's Amateur Radio AX.25 protocol functionality in the way a user connects with the protocol. This flaw allows a local user to crash the syst...
Severity: Medium
Risk Score: 4.7
EPSS Percentile: 5.1%

CVE-2021-3753 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108

Description: A race problem was seen in the vt_k_ioctl in drivers/tty/vt/vt_ioctl.c in the Linux kernel, which may cause an out of bounds read in vt as the write access to vc_mode is not protected by lock-in vt_io...
Severity: Medium
Risk Score: 4.7
EPSS Percentile: 19.7%

CVE-2021-33624 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In kernel/bpf/verifier.c in the Linux kernel before 5.12.13, a branch can be mispredicted (e.g., because of type confusion) and consequently an unprivileged BPF program can read arbitrary memory locat...
Severity: Medium
Risk Score: 4.7
EPSS Percentile: 61.7%

CVE-2020-29372 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in do_madvise in mm/madvise.c in the Linux kernel before 5.6.8. There is a race condition between coredump operations and the IORING_OP_MADVISE implementation, aka CID-bc0c4d1e...
Severity: Medium
Risk Score: 4.7
EPSS Percentile: 32.2%

CVE-2019-19965 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel through 5.4.6, there is a NULL pointer dereference in drivers/scsi/libsas/sas_discover.c because of mishandling of port disconnection during discovery, related to a PHY down race c...
Severity: Medium
Risk Score: 4.7
EPSS Percentile: 40.3%

CVE-2019-16994 🔥 PoC

Reachable

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 5.0, a memory leak exists in sit_init_net() in net/ipv6/sit.c when register_netdev() fails to register sitn->fb_tunnel_dev, which may cause denial of service, aka CID-07f12b...

Severity: Medium
Risk Score: 4.7
EPSS Percentile: 38.7%

CVE-2019-15921 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.0.6. There is a memory leak issue when idr_alloc() fails in genl_register_family() in net/netlink/genetlink.c.
Severity: Medium
Risk Score: 4.7
EPSS Percentile: 40.3%

CVE-2019-15292 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.0.9. There is a use-after-free in atalk_proc_exit, related to net/appletalk/atalk_proc.c, net/appletalk/ddp.c, and net/appletalk/sysctl_net_atalk.c...
Severity: Medium
Risk Score: 4.7
EPSS Percentile: 75.4%

CVE-2019-11190 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The Linux kernel before 4.8 allows local users to bypass ASLR on setuid programs (such as /bin/su) because install_exec_creds() is called too late in load_elf_binary() in fs/binfmt_elf.c, and thus the...
Severity: Medium
Risk Score: 4.7
EPSS Percentile: 19.4%

CVE-2015-5283 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The sctp_init function in net/sctp/protocol.c in the Linux kernel before 4.2.3 has an incorrect sequence of protocol-initialization steps, which allows local users to cause a denial of service (panic ...
Severity: Medium
Risk Score: 4.7
EPSS Percentile: 29.2%

CVE-2014-8086 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: Race condition in the ext4_file_write_iter function in fs/ext4/file.c in the Linux kernel through 3.17 allows local users to cause a denial of service (file unavailability) via a combination of a writ...
Severity: Medium
Risk Score: 4.7
EPSS Percentile: 19.5%

CVE-2014-6410 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The __udf_read_inode function in fs/udf/inode.c in the Linux kernel through 3.16.3 does not restrict the amount of ICB indirection, which allows physically proximate attackers to cause a denial of ser...
Severity: Medium
Risk Score: 4.7
EPSS Percentile: 48.1%

CVE-2013-7339 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The rds_ib_laddr_check function in net/rds/ib.c in the Linux kernel before 3.12.8 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecifi...
Severity: Medium
Risk Score: 4.7
EPSS Percentile: 27.4%

CVE-2013-7026 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: Multiple race conditions in ipc/shm.c in the Linux kernel before 3.12.2 allow local users to cause a denial of service (use-after-free and system crash) or possibly have unspecified other impact via a...
Severity: Medium
Risk Score: 4.7
EPSS Percentile: 5.1%

CVE-2013-6431 🔥 PoC

Reachable

Component: Linux
Version: 3.10.108

Description: The fib6_add function in net/ipv6/ip6_fib.c in the Linux kernel before 3.11.5 does not properly implement error-code encoding, which allows local users to cause a denial of service (NULL pointer deref...
Severity: Medium
Risk Score: 4.7
EPSS Percentile: 13.3%

CVE-2013-6380 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The aac_send_raw_srb function in drivers/scsi/aacraid/commctrl.c in the Linux kernel through 3.12.1 does not properly validate a certain size value, which allows local users to cause a denial of servi...
Severity: Medium
Risk Score: 4.7
EPSS Percentile: 17.9%

CVE-2013-4514 🔥 PoC

Component: Linux
Version: 3.10.108
Description: Multiple buffer overflows in drivers/staging/wlags49_h2/wl_priv.c in the Linux kernel before 3.12 allow local users to cause a denial of service or possibly have unspecified other impact by leveraging...
Severity: Medium
Risk Score: 4.7
EPSS Percentile: 13.4%

CVE-2013-4512 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: Buffer overflow in the exitcode_proc_write function in arch/um/kernel/exitcode.c in the Linux kernel before 3.12 allows local users to cause a denial of service or possibly have unspecified other impa...
Severity: Medium
Risk Score: 4.7
EPSS Percentile: 33.6%

CVE-2023-37453 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the USB subsystem in the Linux kernel through 6.4.2. There is an out-of-bounds and crash in read_descriptors in drivers/usb/core/sysfs.c.
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 40.9%

CVE-2023-25012 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The Linux kernel through 6.1.9 has a Use-After-Free in bigben_remove in drivers/hid/hid-bigbenff.c via a crafted USB device because the LED controllers remain registered for too long.
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 47.7%

CVE-2019-19966 🔥 PoC

Component: Linux
Version: 3.10.108
Description: In the Linux kernel before 5.1.6, there is a use-after-free in cpia2_exit() in drivers/media/usb/cpia2/cpia2_v4l.c that will cause denial of service, aka CID-dea37a972655.
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 48.0%

CVE-2019-15291 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 5.2.9. There is a NULL pointer dereference caused by a malicious USB device in the flexcop_usb_probe function in the drivers/media/usb/b2c2/flexcop-...
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 55.7%

CVE-2019-15223 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.1.8. There is a NULL pointer dereference caused by a malicious USB device in the sound/usb/line6/driver.c driver.
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 51.2%

CVE-2019-15222 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.2.8. There is a NULL pointer dereference caused by a malicious USB device in the sound/usb/helper.c (motu_microbookii) driver.

Severity: Medium
Risk Score: 4.6
EPSS Percentile: 55.8%

CVE-2019-15221 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.1.17. There is a NULL pointer dereference caused by a malicious USB device in the sound/usb/line6/pcm.c driver.
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 48.3%

CVE-2019-15220 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.2.1. There is a use-after-free caused by a malicious USB device in the drivers/net/wireless/intersil/p54/p54usb.c driver.
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 48.3%

CVE-2019-15219 PoC

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.1.8. There is a NULL pointer dereference caused by a malicious USB device in the drivers/usb/misc/sisusbvga/sisusb.c driver.
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 48.3%

CVE-2019-15218 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.1.8. There is a NULL pointer dereference caused by a malicious USB device in the drivers/media/usb/siano/smsusb.c driver.
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 54.0%

CVE-2019-15217 PoC

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.2.3. There is a NULL pointer dereference caused by a malicious USB device in the drivers/media/usb/zr364xx/zr364xx.c driver.
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 48.3%

CVE-2019-15216 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.0.14. There is a NULL pointer dereference caused by a malicious USB device in the drivers/usb/misc/yurex.c driver.
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 48.3%

CVE-2019-15215 🔥 PoC

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.2.6. There is a use-after-free caused by a malicious USB device in the drivers/media/usb/cpia2/cpia2_usb.c driver.
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 48.3%

CVE-2019-15213 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.2.3. There is a use-after-free caused by a malicious USB device in the drivers/media/usb/dvb-usb/dvb-usb-init.c driver.
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 50.0%

CVE-2019-15212 🔥 PoC

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.1.8. There is a double-free caused by a malicious USB device in the drivers/usb/misc/rio500.c driver.
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 48.3%

CVE-2019-15211 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.2.6. There is a use-after-free caused by a malicious USB device in the drivers/media/v4l2-core/v4l2-dev.c driver because drivers/media/radio/radio-...
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 48.3%

CVE-2016-3140 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The digi_port_init function in drivers/usb/serial/digi_acceleport.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and sy...
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 86.6%

CVE-2016-3139 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The wacom_probe function in drivers/input/tablet/wacom_sys.c in the Linux kernel before 3.17 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system cra...
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 83.6%

CVE-2016-3138 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The acm_probe function in drivers/usb/class/cdc-acm.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) vi...
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 61.6%

CVE-2016-3137 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: drivers/usb/serial/cypress_m8.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a USB device without...

Severity: Medium
Risk Score: 4.6
EPSS Percentile: 61.6%

CVE-2016-3136 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The mct_u232_msr_to_state function in drivers/usb/serial/mct_u232.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and sy...
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 86.6%

CVE-2016-2782 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The treo_attach function in drivers/usb/serial/visor.c in the Linux kernel before 4.5 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) or ...
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 74.9%

CVE-2016-2384 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: Double free vulnerability in the snd_usbmidi_create function in sound/usb/midi.c in the Linux kernel before 4.5 allows physically proximate attackers to cause a denial of service (panic) or possibly h...
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 94.2%

CVE-2016-2188 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The iowarrior_probe function in drivers/usb/misc/iowarrior.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system cr...
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 82.6%

CVE-2016-2186 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The powermate_probe function in drivers/input/misc/powermate.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system ...
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 72.2%

CVE-2016-2185 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The ati_remote2_probe function in drivers/input/misc/ati_remote2.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and sys...
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 72.2%

CVE-2016-2184 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The create_fixed_stream_quirk function in sound/usb/quirks.c in the snd-usb-audio driver in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL point...
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 85.3%

CVE-2015-7566 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The clie_5_attach function in drivers/usb/serial/visor.c in the Linux kernel through 4.4.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash...
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 81.6%

CVE-2015-7515 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108

Description: The aiptek_probe function in drivers/input/tablet/aiptek.c in the Linux kernel before 4.4 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash)...
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 76.6%

CVE-2015-5706 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: Use-after-free vulnerability in the path_openat function in fs/namei.c in the Linux kernel 3.x and 4.x before 4.0.4 allows local users to cause a denial of service or possibly have unspecified other i...
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 15.4%

CVE-2014-8989 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The Linux kernel through 3.17.4 does not properly restrict dropping of supplemental group memberships in certain namespace scenarios, which allows local users to bypass intended file permissions by le...
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 5.7%

CVE-2014-4157 🔥 PoC

Component: Linux
Version: 3.10.108
Description: arch/mips/include/asm/thread_info.h in the Linux kernel before 3.14.8 on the MIPS platform does not configure _TIF_SECCOMP checks on the fast system-call path, which allows local users to bypass inten...
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 13.1%

CVE-2013-6432 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The ping_recvmsg function in net/ipv4/ping.c in the Linux kernel before 3.12.4 does not properly interact with read system calls on ping sockets, which allows local users to cause a denial of service ...
Severity: Medium
Risk Score: 4.6
EPSS Percentile: 12.4%

CVE-2021-4032 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A vulnerability was found in the Linux kernel's KVM subsystem in arch/x86/kvm/lapic.c kvm_free_lapic when a failure allocation was detected. In this flaw the KVM subsystem may crash the kernel due to ...
Severity: Medium
Risk Score: 4.4
EPSS Percentile: 41.3%

CVE-2021-4002 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A memory leak flaw in the Linux kernel's hugetlbfs memory usage was found in the way the user maps some regions of memory twice using shmget() which are aligned to PUD alignment with the fault of some...
Severity: Medium
Risk Score: 4.4
EPSS Percentile: 11.8%

CVE-2021-27363 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel through 5.11.3. A kernel pointer leak can be used to determine the address of the iscsi_transport structure. When an iSCSI transport is registered with the ...
Severity: Medium
Risk Score: 4.4
EPSS Percentile: 29.9%

CVE-2020-29660 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: A locking inconsistency issue was discovered in the tty subsystem of the Linux kernel through 5.9.13. drivers/tty/tty_io.c and drivers/tty/tty_jobctrl.c may allow a read-after-free attack against TIOC...
Severity: Medium
Risk Score: 4.4
EPSS Percentile: 33.4%

CVE-2020-25639 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A NULL pointer dereference flaw was found in the Linux kernel's GPU Nouveau driver functionality in versions prior to 5.12-rc1 in the way the user calls ioctl DRM_IOCTL_NOUVEAU_CHANNEL_ALLOC. This fla...
Severity: Medium

Risk Score: 4.4
EPSS Percentile: 31.7%

CVE-2020-15437 🔥 PoC

Reachable

Component: Linux
Version: 3.10.108
Description: The Linux kernel before version 5.8 is vulnerable to a NULL pointer dereference in drivers/tty/serial/8250/8250_core.c:serial8250_isa_init_ports() that allows local users to cause a denial of service ...
Severity: Medium
Risk Score: 4.4
EPSS Percentile: 8.1%

CVE-2019-3701 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in can_can_gw_rcv in net/can/gw.c in the Linux kernel through 4.19.13. The CAN frame modification rules allow bitwise logical operations that can be also applied to the can_dlc...
Severity: Medium
Risk Score: 4.4
EPSS Percentile: 34.4%

CVE-2019-15666 🔥 PoC

Reachable

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.0.19. There is an out-of-bounds array access in __xfrm_policy_unlink, which will cause denial of service, because verify_newpolicy_info in net/xfrm...
Severity: Medium
Risk Score: 4.4
EPSS Percentile: 89.4%

CVE-2019-15031 🔥 PoC

Component: Linux
Version: 3.10.108
Description: In the Linux kernel through 5.2.14 on the powerpc platform, a local user can read vector registers of other users' processes via an interrupt. To exploit the venerability, a local user starts a transa...
Severity: Medium
Risk Score: 4.4
EPSS Percentile: 17.6%

CVE-2019-15030 🔥 PoC

Component: Linux
Version: 3.10.108
Description: In the Linux kernel through 5.2.14 on the powerpc platform, a local user can read vector registers of other users' processes via a Facility Unavailable exception. To exploit the venerability, a local ...
Severity: Medium
Risk Score: 4.4
EPSS Percentile: 24.8%

CVE-2015-7312 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: Multiple race conditions in the Advanced Union Filesystem (aufs) aufs3-mmap.patch and aufs4-mmap.patch patches for the Linux kernel 3.x and 4.x allow local users to cause a denial of service (use-afte...
Severity: Medium
Risk Score: 4.4
EPSS Percentile: 11.0%

CVE-2015-0239 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The em_sysenter function in arch/x86/kvm/emulate.c in the Linux kernel before 3.18.5, when the guest OS lacks SYSENTER MSR initialization, allows guest OS users to gain guest OS privileges or cause a ...
Severity: Medium
Risk Score: 4.4
EPSS Percentile: 47.3%

CVE-2019-15920 🔥 PoC

Component: Linux
Version: 3.10.108
Description: An issue was discovered in the Linux kernel before 5.0.10. SMB2_read in fs/cifs/smb2pdu.c has a use-after-free. NOTE: this was not fixed correctly in 5.0.10; see the 5.0.11 ChangeLog, which documents ...
Severity: Medium
Risk Score: 4.3
EPSS Percentile: 66.9%

CVE-2014-3601 🔥 PoC

Component: Linux
Version: 3.10.108
Description: The kvm_iommu_map_pages function in virt/kvm/iommu.c in the Linux kernel through 3.16.1 miscalculates the number of pages during the handling of a mapping failure, which allows guest OS users to (1) c...
Severity: Medium
Risk Score: 4.3
EPSS Percentile: 58.0%

CVE-2013-4579 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The ath9k_htc_set_bssid_mask function in drivers/net/wireless/ath/ath9k/htc_drv_main.c in the Linux kernel through 3.12 uses a BSSID masking approach to determine the set of MAC addresses on which a W...
Severity: Medium
Risk Score: 4.3
EPSS Percentile: 97.0%

CVE-2020-25656 🔥 PoC

Component: Linux
Version: 3.10.108
Description: A flaw was found in the Linux kernel. A use-after-free was found in the way the console subsystem was using ioctls KDGKBSENT and KDSKBSENT. A local user could use this flaw to get read memory access o...
Severity: Medium
Risk Score: 4.1
EPSS Percentile: 19.5%

CVE-2014-5472 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: The parse_rock_ridge_inode_internal function in fs/isofs/rock.c in the Linux kernel through 3.16.1 allows local users to cause a denial of service (unkillable mount process) via a crafted iso9660 imag...
Severity: Medium
Risk Score: 4.0
EPSS Percentile: 23.7%

CVE-2014-5471 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: Stack consumption vulnerability in the parse_rock_ridge_inode_internal function in fs/isofs/rock.c in the Linux kernel through 3.16.1 allows local users to cause a denial of service (uncontrolled recu...
Severity: Medium
Risk Score: 4.0
EPSS Percentile: 31.5%

CVE-2013-6382 🔥 PoC

Unreachable

Component: Linux
Version: 3.10.108
Description: Multiple buffer underflows in the XFS implementation in the Linux kernel through 3.12.1 allow local

users to cause a denial of service (memory corruption) or possibly have unspecified other impact by ...
Severity: Medium
Risk Score: 4.0
EPSS Percentile: 12.2%

HELPFUL INFORMATION

View this resource to learn more about terms, definitions, and helpful information to understand the firmware risk report.

CORE SECURITY TERMS

Term	Definition
Risk Score	A composite risk score computed by Finite State based on multiple subcomponents and comparison to other binaries. Higher scores indicate greater risk.
Severity	Qualitative risk levels: Critical, High, Medium, Low. Used to categorize the potential impact of security findings.
CVE	Common Vulnerabilities and Exposures - publicly known security vulnerabilities documented in the National Vulnerability Database (NVD).
EPSS Percentile	Exploit Prediction Scoring System percentile (0-100) indicating the likelihood of exploitation compared to all known vulnerabilities. Higher percentiles indicate greater exploitation probability.

COMPONENT AND SOFTWARE TERMS

Term	Definition
Software Bill of Materials (SBOM)	A list of software components found within firmware, including open-source and proprietary components used to assemble the software.
Component	A software component or library that is part of the analyzed firmware or software package.
License	The software license under which a component is distributed, affecting legal and compliance considerations.

EXPLOIT AND THREAT INTELLIGENCE TERMS

Term	Definition
Exploited By Ransomware	Indicates active, high-impact exploitation often resulting in major business disruption.
Exploited By Botnet	Part of mass exploitation campaigns, indicating wide exposure risk.
Exploited By Threat Actors	Known use by real adversaries; strong signal of risk.
In KEV	Listed in CISA Known Exploited Vulnerabilities Catalog based on past exploitation; prioritization recommended by authoritative sources.
Reported in the Wild	Observed being used in attacks, but attribution or scope may be less clear than above.
Commercial Exploit	Available to buyers (e.g., via private brokers); implies advanced threat use.
Weaponized	Packaged in a ready-to-use exploit format (e.g., part of exploit kits or frameworks).
PoC (Proof of Concept)	A working exploit is available, but not necessarily used yet. Still high risk, especially if easy to use.

SECURITY ANALYSIS TERMS

Term	Definition
Credentials	User accounts and credentials found in firmware that can indicate potential backdoors or unauthorized access points.
Crypto Material	Private keys and authorized key files that can indicate backdoors allowing unintended device access.
Exploit Mitigations	Modern software compiler safety features designed to prevent common exploit methods like buffer overflows.

Unsafe Function Calls	Legacy functions (like strcpy) in C that are unsafe and expose binaries to risks like buffer overflow. The platform detects these calls and uses their ratio to total function calls to percentile rank firmware.
Potential Memory Corruptions	Binaries with the highest potential for buffer overflows and other memory-related attacks.
Code Analysis	Static analysis results of source code, identifying security issues like invoking shell commands or command injections. Currently analyzes Python source code.

PROJECT AND VERSION TERMS

Term	Definition
Project	A software project or product being analyzed for security vulnerabilities.
Version	A specific version or release of a project being analyzed.
Finding	A security vulnerability or issue identified during the analysis process.
Violations	Policy violations related to security findings that may require immediate attention.
Warnings	Policy warnings associated with findings that should be reviewed and addressed.