HID: core: zero-initialize the report buffer

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2024-50302
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-11-19 02:16:32 UTC
Updated	2026-05-12 18:47:16 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: HID: core: zero-initialize the report buffer Since the report

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

EPSS: 0.016980000 probability, percentile 0.824110000 (date 2026-05-11)

CISA KEV: Listed on 2025-03-04; due 2025-03-25; ransomware use Unknown

Problem Types: CWE-908 | CWE-908 CWE-908 Use of Uninitialized Resource

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
3.1	ADP	DECLARED	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

CISA Known Exploited Vulnerability

Vendor	Linux
Product	Kernel
Name	Linux Kernel Use of Uninitialized Resource Vulnerability
Required Action	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
Notes	This vulnerability affects a common open-source component, third-party library, or a protocol used by different products. For more information, please see: https://lore.kernel.org/linux-cve-announce/2024111908-CVE-2024-50302-f677@gregkh/ ; https://source.android.com/docs/security/bulletin/2025-03-01 ; https://nvd.nist.gov/vuln/detail/CVE-2024-50302

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Google	Android	-	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Hardware	Siemens	Ruggedcom Rst2428p	-	All	All	All
Hardware	Siemens	Scalance Xc316-8	-	All	All	All
Hardware	Siemens	Scalance Xc319-4	-	All	All	All
Hardware	Siemens	Scalance Xc324-4	-	All	All	All
Hardware	Siemens	Scalance Xc324-4eec	-	All	All	All
Hardware	Siemens	Scalance Xc332	-	All	All	All
Hardware	Siemens	Scalance Xc416-8	-	All	All	All
Hardware	Siemens	Scalance Xc419-4	-	All	All	All
Hardware	Siemens	Scalance Xc424-4	-	All	All	All
Hardware	Siemens	Scalance Xc432	-	All	All	All
Hardware	Siemens	Scalance Xch328	-	All	All	All
Hardware	Siemens	Scalance Xcm324	-	All	All	All
Hardware	Siemens	Scalance Xcm328	-	All	All	All
Hardware	Siemens	Scalance Xcm332	-	All	All	All

Hardware	Siemens	Scalance Xr302-32	-	All	All	All
Hardware	Siemens	Scalance Xr322-12	-	All	All	All
Hardware	Siemens	Scalance Xr326-8	-	All	All	All
Hardware	Siemens	Scalance Xr326-8eec	-	All	All	All
Hardware	Siemens	Scalance Xr502-32	-	All	All	All
Hardware	Siemens	Scalance Xr522-12	-	All	All	All
Hardware	Siemens	Scalance Xr524-8c	-	All	All	All
Hardware	Siemens	Scalance Xr524-8wg	-	All	All	All
Hardware	Siemens	Scalance Xr526-8	-	All	All	All
Hardware	Siemens	Scalance Xr526-8c	-	All	All	All
Hardware	Siemens	Scalance Xr528-6m	-	All	All	All
Hardware	Siemens	Scalance Xr552-12m	-	All	All	All
Hardware	Siemens	Scalance Xrh334	-	All	All	All
Hardware	Siemens	Scalance Xrm334	-	All	All	All
Hardware	Siemens	Simatic S7-1500 Tm Mfp	-	All	All	All
Operating System	Siemens	Simatic S7-1500 Tm Mfp Firmware	-	All	All	All
Operating System	Siemens	Sinec Os	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 27ce405039bfe6d3f4143415c638f56a3df77c
CNA	Linux	Linux	affected 27ce405039bfe6d3f4143415c638f56a3df77c
CNA	Linux	Linux	affected 27ce405039bfe6d3f4143415c638f56a3df77c
CNA	Linux	Linux	affected 27ce405039bfe6d3f4143415c638f56a3df77c
CNA	Linux	Linux	affected 27ce405039bfe6d3f4143415c638f56a3df77c
CNA	Linux	Linux	affected 27ce405039bfe6d3f4143415c638f56a3df77c
CNA	Linux	Linux	affected 27ce405039bfe6d3f4143415c638f56a3df77c
CNA	Linux	Linux	affected 27ce405039bfe6d3f4143415c638f56a3df77c
CNA	Linux	Linux	affected b2b6cadad699d44a8a5b2a60f3d960e00d6fb
CNA	Linux	Linux	affected fe6c9b48ebc920ff21c10c50ab2729440c734
CNA	Linux	Linux	affected 3.12
CNA	Linux	Linux	unaffected 3.12 semver
CNA	Linux	Linux	unaffected 4.19.324 4.19.* semver
CNA	Linux	Linux	unaffected 5.4.286 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.230 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.172 5.15.* semver

CNA	Linux	Linux	unaffected 6.1.117 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.61 6.6.* semver
CNA	Linux	Linux	unaffected 6.11.8 6.11.* semver
CNA	Linux	Linux	unaffected 6.12 * original_commit_for_fix
ADP	Siemens	RUGGEDCOM RST2428P	unaffected * custom
ADP	Siemens	SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family	unaffected * custom
ADP	Siemens	SCALANCE XCM-/XRM-/XCH-/XRH-300 Family	unaffected * custom
ADP	Siemens	SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem	affected * custom

References

Reference	Source	Link
git.kernel.org/stable/c/177f25d1292c7e16e1199b39c85480f7f8815552	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/e7ea60184e1e88a3c9e437b3265cbb6439aa7e26	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/9d9f5c75c0c7f31766ec27d90f7a6ac673193191	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
lists.debian.org/debian-lts-announce/2025/03/msg00002.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/d7dc68d82ab3fcfc3f65322465da3d7031d4ab46	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-265688.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.cc
git.kernel.org/stable/c/1884ab3d22536a5c14b17c78c2ce76d1734e8b0b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/05ade5d4337867929e7ef664e7ac8e0c734f1aaf	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-355557.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.cc
lists.debian.org/debian-lts-announce/2025/01/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/3f9e88f2672c4635960570ee9741778d4135ecf5	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/492015e6249fbcd42138b49de3c588d826dd9648	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0	www.cisa.gov
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2025-03-04T00:00:00.000Z	CVE-2024-50302 added to CISA KEV

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report