firmware_loader: Block path traversal

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

Summary

CVE	CVE-2024-47742
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-10-21 13:15:04 UTC
Updated	2026-05-12 19:07:08 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: firmware_loader: Block path traversal Most firmware name

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

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

Problem Types: CWE-22

CVSS v3.1 Breakdown

Attack Vector
Local

Attack Complexity
Low

Privileges Required
Low

User Interaction
None

Scope
Unchanged

Confidentiality
High

Integrity
High

Availability
High

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

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	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected abb139e75c2cdbb955e840d6331cb5863e409d0e d1768e5535d3ded59f888637016e6f821f4e069f git
CNA	Linux	Linux	affected abb139e75c2cdbb955e840d6331cb5863e409d0e 9b1ca33ebd05b3acef5b976c04e5e791af93ce1b gi
CNA	Linux	Linux	affected abb139e75c2cdbb955e840d6331cb5863e409d0e c30558e6c5c9ad6c86459d9acce1520ceeab9ea6 g
CNA	Linux	Linux	affected abb139e75c2cdbb955e840d6331cb5863e409d0e a77fc4acfd49fc6076e565445b2bc5fdc3244da4 git
CNA	Linux	Linux	affected abb139e75c2cdbb955e840d6331cb5863e409d0e 3d2411f4edcb649eaf232160db459bb4770b5251 g
CNA	Linux	Linux	affected abb139e75c2cdbb955e840d6331cb5863e409d0e 7420c1bf7fc784e587b87329cc6dfa3dca537aa4 git
CNA	Linux	Linux	affected abb139e75c2cdbb955e840d6331cb5863e409d0e 28f1cd94d3f1092728fb775a0fe26c5f1ac2ebeb git
CNA	Linux	Linux	affected abb139e75c2cdbb955e840d6331cb5863e409d0e 6c4e13fdfcab34811c3143a0a03c05fec4e870ec git
CNA	Linux	Linux	affected abb139e75c2cdbb955e840d6331cb5863e409d0e f0e5311aa8022107d63c54e2f03684ec097d1394 g
CNA	Linux	Linux	affected 3.7
CNA	Linux	Linux	unaffected 3.7 semver
CNA	Linux	Linux	unaffected 4.19.323 4.19.* semver
CNA	Linux	Linux	unaffected 5.4.285 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.227 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.168 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.113 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.54 6.6.* semver
CNA	Linux	Linux	unaffected 6.10.13 6.10.* semver
CNA	Linux	Linux	unaffected 6.11.2 6.11.* semver
CNA	Linux	Linux	unaffected 6.12 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/6c4e13fdfcab34811c3143a0a03c05fec4e870ec	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/c30558e6c5c9ad6c86459d9acce1520ceeab9ea6	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/7420c1bf7fc784e587b87329cc6dfa3dca537aa4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
lists.debian.org/debian-lts-announce/2025/03/msg00002.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	Maili
git.kernel.org/stable/c/3d2411f4edcb649eaf232160db459bb4770b5251	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/d1768e5535d3ded59f888637016e6f821f4e069f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc

git.kernel.org/stable/c/a77fc4acfd49fc6076e565445b2bc5fdc3244da4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/f0e5311aa8022107d63c54e2f03684ec097d1394	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/9b1ca33ebd05b3acef5b976c04e5e791af93ce1b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
lists.debian.org/debian-lts-announce/2025/01/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	Maili
git.kernel.org/stable/c/28f1cd94d3f1092728fb775a0fe26c5f1ac2ebeb	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

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