



# firmware\_loader: Block path traversal

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2024-47742
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-10-21 13:15:04 UTC
<b>Updated</b>	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	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected <a href="#">abb139e75c2cdbb955e840d6331cb5863e409d0e</a> <a href="#">d1768e5535d3ded59f888637016e6f821f4e069f</a> git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected <a href="#">abb139e75c2cdbb955e840d6331cb5863e409d0e</a> <a href="#">9b1ca33ebd05b3acef5b976c04e5e791af93ce1b</a> git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected <a href="#">abb139e75c2cdbb955e840d6331cb5863e409d0e</a> <a href="#">c30558e6c5c9ad6c86459d9acce1520ceeab9ea6</a> git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected <a href="#">abb139e75c2cdbb955e840d6331cb5863e409d0e</a> <a href="#">a77fc4acfd49fc6076e565445b2bc5fdc3244da4</a> git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected <a href="#">abb139e75c2cdbb955e840d6331cb5863e409d0e</a> <a href="#">3d2411f4edcb649eaf232160db459bb4770b5251</a> git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected <a href="#">abb139e75c2cdbb955e840d6331cb5863e409d0e</a> <a href="#">7420c1bf7fc784e587b87329cc6dfa3dca537aa4</a> git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected <a href="#">abb139e75c2cdbb955e840d6331cb5863e409d0e</a> <a href="#">28f1cd94d3f1092728fb775a0fe26c5f1ac2ebeb</a> git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected <a href="#">abb139e75c2cdbb955e840d6331cb5863e409d0e</a> <a href="#">6c4e13fdcab34811c3143a0a03c05fec4e870ec</a> git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected <a href="#">abb139e75c2cdbb955e840d6331cb5863e409d0e</a> <a href="#">f0e5311aa8022107d63c54e2f03684ec097d1394</a> git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 3.7
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 3.7 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 4.19.323 4.19.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.4.285 5.4.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.10.227 5.10.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.15.168 5.15.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.1.113 6.1.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.54 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.10.13 6.10.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.11.2 6.11.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12 * original_commit_for_fix

## References

Reference	Source	Link	Tags
<a href="#">git.kernel.org/stable/c/6c4e13fdcab34811c3143a0a03c05fec4e870ec</a>	<a href="#">416baaa9-dc9f-4396-8d5f-8c081fb06d67</a>	<a href="#">git.kernel.org</a>	Patc
<a href="#">git.kernel.org/stable/c/c30558e6c5c9ad6c86459d9acce1520ceeab9ea6</a>	<a href="#">416baaa9-dc9f-4396-8d5f-8c081fb06d67</a>	<a href="#">git.kernel.org</a>	Patc
<a href="#">git.kernel.org/stable/c/7420c1bf7fc784e587b87329cc6dfa3dca537aa4</a>	<a href="#">416baaa9-dc9f-4396-8d5f-8c081fb06d67</a>	<a href="#">git.kernel.org</a>	Patc
<a href="#">lists.debian.org/debian-lts-announce/2025/03/msg00002.html</a>	<a href="#">af854a3a-2127-422b-91ae-364da2661108</a>	<a href="#">lists.debian.org</a>	Maili
<a href="#">git.kernel.org/stable/c/3d2411f4edcb649eaf232160db459bb4770b5251</a>	<a href="#">416baaa9-dc9f-4396-8d5f-8c081fb06d67</a>	<a href="#">git.kernel.org</a>	Patc
<a href="#">git.kernel.org/stable/c/d1768e5535d3ded59f888637016e6f821f4e069f</a>	<a href="#">416baaa9-dc9f-4396-8d5f-8c081fb06d67</a>	<a href="#">git.kernel.org</a>	Patc

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

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)