



platform/x86: panasonic-laptop: Fix SINF array out of bounds accesses

[MITRE](#)

[NVD](#)

[CVE.ORG](#)

[JSON API](#)

[Print: PDF](#)

Summary

CVE	CVE-2024-46859
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-09-27 13:15:17 UTC
Updated	2026-05-05 15:06:23 UTC

Description In the Linux kernel, the following vulnerability has been resolved: platform/x86: panasonic-laptop: Fix SINF array out of bounds accesses

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-129

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 e424fb8cc4e6634c10f8159b1ff5618cf7bab9c6 b7c2f692307fe704be87ea80d7328782b33c3cef git
CNA	Linux	Linux	affected e424fb8cc4e6634c10f8159b1ff5618cf7bab9c6 9291fadb2720a869b1d2fcf82305648e2e62a16 git
CNA	Linux	Linux	affected e424fb8cc4e6634c10f8159b1ff5618cf7bab9c6 6821a82616f60aa72c5909b3e252ad97fb9f7e2a git
CNA	Linux	Linux	affected e424fb8cc4e6634c10f8159b1ff5618cf7bab9c6 b38c19783286a71693c2194ed1b36665168c09c4 git
CNA	Linux	Linux	affected e424fb8cc4e6634c10f8159b1ff5618cf7bab9c6 f52e98d16e9bd7dd2b3aef8e38db5cbc9899d6a4 git
CNA	Linux	Linux	affected 3.3
CNA	Linux	Linux	unaffected 3.3 semver
CNA	Linux	Linux	unaffected 5.15.168 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.111 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.52 6.6.* semver
CNA	Linux	Linux	unaffected 6.10.11 6.10.* semver
CNA	Linux	Linux	unaffected 6.11 * original_commit_for_fix

References				
Reference	Source	Link	Tag	
git.kernel.org/stable/c/6821a82616f60aa72c5909b3e252ad97fb9f7e2a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc	
git.kernel.org/stable/c/b38c19783286a71693c2194ed1b36665168c09c4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc	
git.kernel.org/stable/c/f52e98d16e9bd7dd2b3aef8e38db5cbc9899d6a4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc	
git.kernel.org/stable/c/9291fadb2720a869b1d2fcf82305648e2e62a16	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	Mail	
git.kernel.org/stable/c/b7c2f692307fe704be87ea80d7328782b33c3cef	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.

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)