

CVE-2022-0185

Linux Kernel Heap-Based Buffer Overflow Vulnerability

CISA KEV since Aug 21, 2024

Actively exploited

A heap-based buffer overflow flaw was found in the way the legacy_parse_param function in the Filesystem Context functionality of the Linux kernel verified the supplied parameters length. An unprivileged (in case of unprivileged user namespaces enabled, otherwise needs namespaced CAP_SYS_ADMIN privilege) local user able to open a filesystem that does not support the Filesystem Context API (and thus fallbacks to legacy handling) could use this flaw to escalate their privileges on the system.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 8.4 High · NVD	EPSS 0.252 97.9th percentile · FIRST	CISA DEADLINE Sep 11, 2024 KEV since 2024 · listed over a year
--	---------------------------------------	---	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.252 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.4	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions or discontinue use of the product if updates are unavailable. **CISA note:** This vulnerability affects a common open-source component, third-party library, or a protocol used by different products.
Basis: CISA KEV required action

Affected and fixed versions · 9 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
linux kernel	≥ 5.1 < 5.4.173 ≥ 5.5 < 5.10.93 ≥ 5.11 < 5.15.16 ≥ 5.16 < 5.16.2	no fixed version listed	NVD
h410c firmware	—	no fixed version listed	NVD
h300s firmware	—	no fixed version listed	NVD
h500s firmware	—	no fixed version listed	NVD
h700s firmware	—	no fixed version listed	NVD
h300e firmware	—	no fixed version listed	NVD
h500e firmware	—	no fixed version listed	NVD
h700e firmware	—	no fixed version listed	NVD

Sources

Vendor guidance git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit?id=722d94847de2
NVD nvd.nist.gov/vuln/detail/CVE-2022-0185
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2022-15389

git.kernel.org git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit?id=722d94847de2
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2022-0185

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.