

# CVE-2024-1086

## Linux Kernel Use-After-Free Vulnerability

CISA KEV since May 30, 2024

Actively exploited

Ransomware use known

A use-after-free vulnerability in the Linux kernel's netfilter: nf\_tables component can be exploited to achieve local privilege escalation. The nft\_verdict\_init() function allows positive values as drop error within the hook verdict, and hence the nf\_hook\_slow() function can cause a double free vulnerability when NF\_DROP is issued with a drop error which resembles NF\_ACCEPT. We recommend upgrading past commit f342de4e2f33e0e39165d8639387aa6c19dff660.

EVRS

75/100

Urgent priority

CVSS V3.1

7.8

High · NVD

EPSS

0.281

98.1st percentile · FIRST

CISA DEADLINE

Jun 20, 2024

KEV since 2024 · listed over a year

### Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

|                                                |                            |                                                         |                                            |
|------------------------------------------------|----------------------------|---------------------------------------------------------|--------------------------------------------|
| <input checked="" type="checkbox"/> CISA KEV   | Listed in the catalog      | <input type="checkbox"/> Vendor exploitation            | Confirmed exploitation in the wild         |
| <input checked="" type="checkbox"/> Ransomware | Known ransomware campaigns | <input type="checkbox"/> KEV recency                    | On the CISA KEV catalog for over two years |
| <input checked="" type="checkbox"/> EPSS       | 0.281 probability          | <input type="checkbox"/> Pre-patch disclosure           | Disclosure status unavailable              |
| <input checked="" type="checkbox"/> CVSS       | Base score 7.8             | <input type="checkbox"/> Microsoft Exploitability Index | Not a Microsoft CVE                        |

### Remediation

**Patch This Cycle** Patch or fixed version identified

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

Please check with specific vendors for information on patching status.

Basis: CISA KEV required action

### Affected and fixed versions · 19 more affected products on the NVD record

| PACKAGE        | AFFECTED                                                                      | FIXED IN                | SOURCE |
|----------------|-------------------------------------------------------------------------------|-------------------------|--------|
| h300s firmware | –                                                                             | no fixed version listed | NVD    |
| h500s firmware | –                                                                             | no fixed version listed | NVD    |
| h700s firmware | –                                                                             | no fixed version listed | NVD    |
| h410s firmware | –                                                                             | no fixed version listed | NVD    |
| h410c firmware | –                                                                             | no fixed version listed | NVD    |
| bootstrap os   | –                                                                             | no fixed version listed | NVD    |
| linux kernel   | ≥ 3.15 < 5.15.149<br>≥ 6.1 < 6.1.76<br>≥ 6.2 < 6.6.15<br>≥ 6.7 < 6.7.3<br>6.8 | no fixed version listed | NVD    |
| fedora         | 39                                                                            | no fixed version listed | NVD    |

## Sources

|                 |                                                                                                                                                                                                                                                   |            |                                                                                                                             |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-----------------------------------------------------------------------------------------------------------------------------|
| Vendor guidance | <a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit?id=f342de4e2f33e0e39165d8639387aa6c19dff660">git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit?id=f342de4e2f33e0e39165d8639387aa6c19dff660</a> | NVD        | <a href="https://nvd.nist.gov/vuln/detail/CVE-2024-1086">nvd.nist.gov/vuln/detail/CVE-2024-1086</a>                         |
| CISA KEV        | <a href="https://cisa.gov/known-exploited-vulnerabilities-catalog">cisa.gov/known-exploited-vulnerabilities-catalog</a>                                                                                                                           | ENISA EUVD | <a href="https://euvd.enisa.europa.eu/vulnerability/EUVD-2024-16861">euvd.enisa.europa.eu/vulnerability/EUVD-2024-16861</a> |
| Current data    | <a href="https://evulnable.com/vulnerability-management/cve/CVE-2024-1086">evulnable.com/vulnerability-management/cve/CVE-2024-1086</a>                                                                                                           |            |                                                                                                                             |

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