

# CVE-2023-0386

## Linux Kernel Improper Ownership Management Vulnerability

CISA KEV since Jun 17, 2025

Actively exploited

Public exploit module (Metasploit)

A flaw was found in the Linux kernel, where unauthorized access to the execution of the setuid file with capabilities was found in the Linux kernel's OverlayFS subsystem in how a user copies a capable file from a nosuid mount into another mount. This uid mapping bug allows a local user to escalate their privileges on the system.

|                                                                |                                                      |                                                                  |                                                                                           |
|----------------------------------------------------------------|------------------------------------------------------|------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| <p>EVRS</p> <p><b>75</b>/100</p> <p><b>Urgent</b> priority</p> | <p>CVSS V3.1</p> <p><b>7.8</b></p> <p>High · NVD</p> | <p>EPSS</p> <p><b>0.079</b></p> <p>94.7th percentile · FIRST</p> | <p>CISA DEADLINE</p> <p><b>Jul 8, 2025</b></p> <p>KEV since 2025 · listed over a year</p> |
|----------------------------------------------------------------|------------------------------------------------------|------------------------------------------------------------------|-------------------------------------------------------------------------------------------|

### Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

|                                                     |                                          |                                                                |                                             |
|-----------------------------------------------------|------------------------------------------|----------------------------------------------------------------|---------------------------------------------|
| <input checked="" type="checkbox"/> <b>CISA KEV</b> | Listed in the catalog                    | <input type="checkbox"/> <b>Vendor exploitation</b>            | Confirmed exploitation in the wild          |
| <input type="checkbox"/> <b>Ransomware</b>          | No known ransomware campaign association | <input type="checkbox"/> <b>KEV recency</b>                    | Added to CISA KEV within the last two years |
| <input checked="" type="checkbox"/> <b>EPSS</b>     | 0.079 probability                        | <input type="checkbox"/> <b>Pre-patch disclosure</b>           | Disclosure status unavailable               |
| <input checked="" type="checkbox"/> <b>CVSS</b>     | Base score 7.8                           | <input type="checkbox"/> <b>Microsoft Exploitability Index</b> | Not a Microsoft CVE                         |

### Remediation

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

**CISA required action:** Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, 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.

Basis: CISA KEV required action

### Affected and fixed versions · 5 more affected products on the NVD record

| PACKAGE        | AFFECTED                                  | FIXED IN                | SOURCE |
|----------------|-------------------------------------------|-------------------------|--------|
| debian linux   | 10.0                                      | 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    |
| h410s firmware | —                                         | no fixed version listed | NVD    |
| h410c firmware | —                                         | no fixed version listed | NVD    |
| ubuntu linux   | 18.04<br>20.04<br>22.04                   | no fixed version listed | NVD    |
| linux kernel   | ≥ 5.11 < 5.15.91<br>≥ 5.16 < 6.1.9<br>6.2 | no fixed version listed | NVD    |



## Sources

|                     |                                                                                                                                                                                             |                   |                                                                                                                             |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Vendor guidance     | <a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=4f11ada10d0a">git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=4f11ada10d0a</a> | access.redhat.com | <a href="https://access.redhat.com/security/cve/cve-2023-0386">access.redhat.com/security/cve/cve-2023-0386</a>             |
| security.netapp.com | <a href="https://security.netapp.com/advisory/ntap-20230420-0004/">security.netapp.com/advisory/ntap-20230420-0004/</a>                                                                     | NVD               | <a href="https://nvd.nist.gov/vuln/detail/CVE-2023-0386">nvd.nist.gov/vuln/detail/CVE-2023-0386</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-2023-12447">euvd.enisa.europa.eu/vulnerability/EUVD-2023-12447</a> |
| Current data        | <a href="https://evulnable.com/vulnerability-management/cve/CVE-2023-0386">evulnable.com/vulnerability-management/cve/CVE-2023-0386</a>                                                     |                   |                                                                                                                             |

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