

# CVE-2022-0995

## Linux Kernel Out-of-Bounds Write Vulnerability

CISA KEV since Aug 26, 2026

Actively exploited

Public exploit module (Metasploit)

An out-of-bounds (OOB) memory write flaw was found in the Linux kernel's watch\_queue event notification subsystem. This flaw can overwrite parts of the kernel state, potentially allowing a local user to gain privileged access or cause a denial of service on the system.

|                                                       |                                       |                                                   |                                                                                    |
|-------------------------------------------------------|---------------------------------------|---------------------------------------------------|------------------------------------------------------------------------------------|
| EVRS<br><b>75</b> / <sub>100</sub><br>Urgent priority | CVSS V3.1<br><b>7.8</b><br>High · NVD | EPSS<br><b>0.089</b><br>95.2nd percentile · FIRST | CISA DEADLINE<br><b>Aug 29, 2026</b><br>CISA federal deadline · Overdue by 54 days |
|-------------------------------------------------------|---------------------------------------|---------------------------------------------------|------------------------------------------------------------------------------------|

### 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 checked="" type="checkbox"/> <b>KEV recency</b>         | Added to CISA KEV within the last 90 days |
| <input checked="" type="checkbox"/> <b>EPSS</b>     | 0.089 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 in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines. **CISA note:** This vulnerability affects an open-source component, third-party library, protocol, or proprietary implementation that could be used by different products.

Basis: CISA KEV required action

### Affected and fixed versions · 16 more affected products on the NVD record

| PACKAGE        | AFFECTED                                                        | FIXED IN                | SOURCE |
|----------------|-----------------------------------------------------------------|-------------------------|--------|
| linux kernel   | ≥ 5.8 < 5.10.106<br>≥ 5.11 < 5.15.29<br>≥ 5.16 < 5.16.5<br>5.17 | no fixed version listed | NVD    |
| fedora         | 35                                                              | no fixed version listed | NVD    |
| h300e firmware | —                                                               | no fixed version listed | NVD    |
| h300s firmware | —                                                               | no fixed version listed | NVD    |
| h410c firmware | —                                                               | no fixed version listed | NVD    |
| h410s firmware | —                                                               | no fixed version listed | NVD    |
| h500e firmware | —                                                               | no fixed version listed | NVD    |
| h500s firmware | —                                                               | no fixed version listed | NVD    |

## Sources

|                        |                                                                                                                                                                                             |                                      |                                                                                                                                                                                                                                                     |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Vendor guidance</b> | <a href="https://bugzilla.redhat.com/show_bug.cgi?id=2063786">bugzilla.redhat.com/show_bug.cgi?id=2063786</a>                                                                               | <b>Additional guidance</b>           | <a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=93ce93587d36493f2f86921fa79921b3cba63fbb">git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=93ce93587d36493f2f86921fa79921b3cba63fbb</a> |
| <b>BOD 26-04</b>       | <a href="https://cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk">cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk</a> | <b>Forensics Triage Requirements</b> | <a href="https://cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk">cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk</a>         |
| <b>NVD</b>             | <a href="https://nvd.nist.gov/vuln/detail/CVE-2022-0995">nvd.nist.gov/vuln/detail/CVE-2022-0995</a>                                                                                         | <b>CISA KEV</b>                      | <a href="https://cisa.gov/known-exploited-vulnerabilities-catalog">cisa.gov/known-exploited-vulnerabilities-catalog</a>                                                                                                                             |
| <b>ENISA EUVD</b>      | <a href="https://euvd.enisa.europa.eu/vulnerability/EUVD-2022-15988">euvd.enisa.europa.eu/vulnerability/EUVD-2022-15988</a>                                                                 | <b>Current data</b>                  | <a href="https://evulnable.com/vulnerability-management/cve/CVE-2022-0995">evulnable.com/vulnerability-management/cve/CVE-2022-0995</a>                                                                                                             |

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