

# CVE-2025-34026

## Versa Concerto Improper Authentication Vulnerability

CISA KEV since Jan 22, 2026

Actively exploited

The Versa Concerto SD-WAN orchestration platform is vulnerable to an authentication bypass in the Traefik reverse proxy configuration, allowing an attacker to access administrative endpoints. The internal Actuator endpoint can be leveraged for access to heap dumps and trace logs. This issue is known to affect Concerto from 12.1.2 through 12.2.0. Additional versions may be vulnerable.

|                                                                |                                                          |                                                                   |                                                                                                    |
|----------------------------------------------------------------|----------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| <p>EVRS</p> <p><b>84</b>/100</p> <p><b>Urgent</b> priority</p> | <p>CVSS V4.0</p> <p><b>9.2</b></p> <p>Critical · NVD</p> | <p>EPSS</p> <p><b>0.818</b></p> <p>99.65th percentile · FIRST</p> | <p>CISA DEADLINE</p> <p><b>Feb 12, 2026</b></p> <p>CISA federal deadline · Overdue by 8 months</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 year |
| <input checked="" type="checkbox"/> <b>EPSS</b>     | 0.818 probability                        | <input type="checkbox"/> <b>Pre-patch disclosure</b>           | Disclosure status unavailable          |
| <input checked="" type="checkbox"/> <b>CVSS</b>     | Base score 9.2                           | <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.

Basis: CISA KEV required action

### Affected and fixed versions

| PACKAGE  | AFFECTED                              | FIXED IN | SOURCE |
|----------|---------------------------------------|----------|--------|
| concerto | ≥ 11.4.0 < 12.1.2<br>12.1.2<br>12.2.0 | 12.1.2   | NVD    |

### Sources

**Vendor guidance** [github.com/advisories/GHSA-h2mm-jj4p-hm2p](https://github.com/advisories/GHSA-h2mm-jj4p-hm2p)

**NVD** [nvd.nist.gov/vuln/detail/CVE-2025-34026](https://nvd.nist.gov/vuln/detail/CVE-2025-34026)

**ENISA EUVD** [euvd.enisa.europa.eu/vulnerability/EUVD-2025-16087](https://euvd.enisa.europa.eu/vulnerability/EUVD-2025-16087)

**Additional guidance** [security-portal.versa-networks.com/emailbulletins/6830f94328defa375486ff2e](https://security-portal.versa-networks.com/emailbulletins/6830f94328defa375486ff2e)

**CISA KEV** [cisa.gov/known-exploited-vulnerabilities-catalog](https://cisa.gov/known-exploited-vulnerabilities-catalog)

**Current data** [evulnable.com/vulnerability-management/cve/CVE-2025-34026](https://evulnable.com/vulnerability-management/cve/CVE-2025-34026)

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