CISA Adds Exploited GitLab and Cisco Flaws to KEV Catalogue



CISA has added two actively exploited flaws in Cisco and GitLab software to its KEV catalogue. One, CVE-2026-97229 in GitLab, carries a CVSS score of 10.0. The source excerpt gives few further details.

- CISA added two Cisco and GitLab flaws to its Known Exploited Vulnerabilities (KEV) catalogue.
- The listing is based on evidence of active exploitation.
- CVE-2026-97229 is an integer overflow or wraparound flaw in GitLab Community Edition and Enterprise, scored CVSS 10.0.
- The headline describes the GitLab issue as remote code execution and the Cisco issue as a firewall denial of service.
- The source excerpt does not give the second CVE number or patch details.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added two vulnerabilities affecting Cisco and GitLab software to its Known Exploited Vulnerabilities (KEV) catalogue, citing evidence that they are being exploited in the wild.

What is known

The first entry is **CVE-2026-97229**, an integer overflow or wraparound vulnerability in GitLab Community Edition and Enterprise, with a CVSS score of 10.0. According to the source headline, the GitLab flaw allows remote code execution, while the Cisco flaw is a denial-of-service issue affecting firewalls.

The excerpt available to us does not include the Cisco CVE identifier, the affected versions or the fixed releases. We therefore do not describe those details here and recommend checking the vendor advisories directly.

Why it matters

A KEV listing signals that exploitation has been observed, which moves a vulnerability from theoretical risk to an operational priority. A maximum-score flaw in a source-code platform is of particular interest, since such platforms often hold code, credentials and pipeline access. A denial-of-service flaw in a perimeter firewall can affect availability of protected services.

Institutions running either product should confirm exposure and follow the vendors' guidance without waiting for further reporting.

What to do now

1. Identify all GitLab Community Edition and Enterprise instances and Cisco firewalls in your estate, including internet-facing ones.
2. Review the GitLab and Cisco vendor advisories for CVE-2026-97229 and the Cisco flaw, and apply fixes or mitigations as directed.
3. Prioritise the GitLab instances, given the CVSS 10.0 score and confirmed exploitation.
4. Check GitLab and firewall logs for unusual activity, and rotate secrets stored in affected GitLab instances if compromise is suspected.
5. Add KEV monitoring to your vulnerability management process and record patch decisions for audit.