CISA adds 10 exploited flaws to KEV catalog, including five in Mitel MiCollab



CISA has added 10 vulnerabilities to its Known Exploited Vulnerabilities catalog, five of them in Mitel MiCollab and disclosed the week before. The source headline also names Juniper, Vates and Danfoss products.

- CISA added 10 security flaws to its KEV catalog on Wednesday.
- Five of them affect Mitel MiCollab and were disclosed the previous week.
- One listed Mitel flaw, CVE-2026-133275 (CVSS 5.3), is an arbitrary file upload issue.
- The headline indicates Juniper, Vates and Danfoss products are also affected.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added 10 vulnerabilities to its **Known Exploited Vulnerabilities (KEV)** catalog. Inclusion in the catalog means exploitation has been observed, so

these flaws deserve priority over issues that are only theoretical.

What was reported

Five of the additions affect Mitel MiCollab, a collaboration product, and were disclosed only a week earlier. One of them, CVE-2026-133275, carries a CVSS score of 5.3 and is an arbitrary file upload vulnerability in a component of the product. The source headline also refers to Juniper, Vates and Danfoss products among the affected vendors.

The excerpt available to us does not list the remaining CVE identifiers, affected versions or patch details, so these should be confirmed against the vendors' own advisories and the CISA catalog entries.

Why it matters

A moderate CVSS score should not lower the priority of a flaw that is known to be exploited. Exploitation status is often a better guide to urgency than the score alone. Organisations running any of the named products, especially systems reachable from the internet, should check their exposure now.

Suggested approach

Start with an inventory check for the named vendors, then apply vendor fixes or mitigations where available, and review logs for signs of abuse before and after patching.

What to do now

1. Check asset inventories for Mitel MiCollab, Juniper, Vates and Danfoss products.
2. Retrieve the full list of the 10 CVEs from the CISA KEV catalog and vendor advisories.
3. Prioritise patching or mitigating exposed MiCollab instances, regardless of the moderate CVSS score.
4. Review logs on affected systems for suspicious file uploads or unexpected activity.
5. Add KEV catalog monitoring to the vulnerability management process.