Mitel MiCollab, Juniper Session Smart, Xen Orchestra and Danfoss AK-SM 800A exploited flaws (CVE-2026-133323 and 9 others)

Status: Recovering / monitoring

Started Nov 28, 2026, 11:29 AM PST · Multiple (Mitel, HPE Juniper Networks, Vates, Danfoss)'s estimate: Fixed versions are available

CVE-2026-133275, CVE-2026-133303, CVE-2026-133311, CVE-2026-133323, CVE-2026-133324, CVE-2026-103406, CVE-2026-133469, CVE-2023-25914, CVE-2023-25915, CVE-2025-41450 · CVSS 9.8 (critical) · Being exploited: yes · Fix available: yes

WHAT'S HAPPENING

CISA keeps a public list of security flaws that attackers are known to be using. On November 25, 2026 it added 10 entries from four unrelated products. CISA does not link the four vendors to one campaign. Five entries are in the conferencing component of Mitel MiCollab, a business phone and collaboration system. Mitel says the file-upload flaw (CVE-2026-133275) could let an unauthenticated attacker upload files because the file type is not checked properly. Mitel's advisory also says another flaw could let an attacker run commands on the system. One entry is a Juniper Session Smart Conductor flaw (CVE-2026-103406). It could let attackers run commands with root (full administrator) privileges. One is a Xen Orchestra login bypass (CVE-2026-133469). Vates says it uses a crafted cookie to act as an administrator. Three are older flaws in Danfoss AK-SM 800A refrigeration controllers. Danfoss fixed these in earlier firmware, but CISA now says they are being exploited. Most of these products are business or industrial equipment, so ordinary home users are unlikely to be running them.

WHO IS AFFECTED

- Mitel MiCollab: <cite index="12-7">version 10.3 (10.3.0.18) and earlier</cite> (conferencing component, called AWV).
- Juniper Session Smart Conductor: <cite index="39-6">versions before 7.0.5, 7.1.0 up to before 7.1.7, and 7.2.0 up to before 7.2.3.</cite> CISA's entry also names Session Smart Router, and the fixed releases are the same.
- Vates Xen Orchestra and Xen Orchestra Appliance: <cite index="43-3">versions before 6.9.2 (stable channel) or 6.10.1 (latest channel).</cite>
- Danfoss AK-SM 800A Series: per public reporting, firmware older than 3.3 (CVE-2023-25914 and CVE-2023-25915) and older than R4.2 (CVE-2025-41450). <cite index="51-3">CISA's 2025 advisory confirms the R4.2 detail for CVE-2025-41450.</cite> I could not confirm the 3.3 detail from Danfoss itself.

IS IT BEING EXPLOITED?

CISA added the 10 vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog on November 25, 2026, based on evidence of active exploitation. For Juniper, the vendor said at least one malicious exploitation had been reported to its security team. For Xen Orchestra, Vates said the flaw was actively exploited by a threat actor when it published its advisory on November 10, 2026. CISA's alert gives no attack details for the Mitel and Danfoss entries. Whether ransomware gangs are using any of them is not confirmed. The score shown (9.8) is the highest one I could confirm, for the Juniper flaw. Some press reports put the worst Mitel flaw at 10.0, but I could not confirm that from an official source.

WHAT YOU SHOULD DO NOW

Home users

• These are business and industrial products. Most households don't run them, and no action is needed if you don't.

• If you use a business phone or conferencing system provided by an employer or IT provider, ask them whether it is Mitel MiCollab and whether it has been updated.

• If you run a home lab with Xen Orchestra or XCP-ng, update Xen Orchestra to 6.9.2 (stable) or 6.10.1 (latest), and don't expose it directly to the internet.

Businesses

• Make a list of any Mitel MiCollab, Juniper Session Smart, Xen Orchestra or Danfoss AK-SM controllers you own, including ones managed by vendors or IT providers.

• Mitel MiCollab: apply the Mitel patch for release 10.3 (10.3.0.18), described in knowledge-base article KB000129195, or move to a later release. Until then, <cite index="6-8">restrict external access to the AWV component.</cite>

• Juniper: upgrade Session Smart Conductor and Router to 7.0.5, 7.1.7, 7.2.3 or later. <cite index="30-13">Juniper says there is no workaround for CVE-2026-103406.</cite>

• Xen Orchestra: upgrade to 6.9.2 or 6.10.1 or later. Move it off the public internet, onto a management network, VPN or approved-address list. <cite index="42-12">Vates notes the unauthenticated access leaves no log entry in Xen Orchestra,</cite> so look for signs of compromise using the indicators in Vates' advisory (VSA-2026-062). If you suspect a compromise, <cite index="42-11">rotate all passwo

• Danfoss AK-SM 800A: upgrade the firmware using Danfoss's software upgrade process, and keep controllers off direct internet exposure. Separately, <cite index="53-1">older Danfoss AK-SM 800 and AK-SC 355 models are end-of-life, so security patches may no longer be available.</cite> Isolate those units and plan to replace them.

• Because several of these flaws were exploited before or soon after their patches came out, patching alone may not be enough. Have your IT provider check for signs of intrusion, such as unexpected files, new accounts or unusual outbound traffic, especially on internet-facing MiCollab and Xen Orchestra servers.

HOW TO CHECK IF YOU'RE AFFECTED

• Mitel MiCollab: sign in to the MiCollab administration page and check the installed version and patch level. Compare it with Mitel advisory MISA-2026-0012. Versions 10.3 (10.3.0.18) and earlier need the patch.

• Juniper Session Smart: on the Conductor or Router, check the software version (for example with the show system version command, or the version shown in the web interface). Compare it with 7.0.5, 7.1.7 and 7.2.3.

• Xen Orchestra: the version appears in the web interface, in the About or Settings area. Appliance (XOA) users can also run the update tool. Check that it shows 6.9.2 (stable) or 6.10.1 (latest) or newer.

• Danfoss AK-SM 800A: the firmware version is shown in the controller's web interface. Compare it with the fixed versions in the 'Fixed versions' list. Ask your refrigeration or facilities contractor if you aren't sure.

• Not sure which of these you use? Ask your IT provider for an inventory of internet-facing systems.

FIXED VERSIONS AND WORKAROUNDS

• Mitel MiCollab (CVE-2026-133275, -133303, -133311, -133323, -133324): Patch for release 10.3 (10.3.0.18) (KB000129195), or a later release

• Juniper Session Smart Conductor / Router (CVE-2026-103406): 7.0.5, 7.1.7 or 7.2.3 (or later)

• Vates Xen Orchestra (CVE-2026-133469): 6.9.2 (stable) or 6.10.1 (latest), or later

• Danfoss AK-SM 800A (CVE-2025-41450): Release R4.2 or later

• Danfoss AK-SM 800A (CVE-2023-25914, CVE-2023-25915): Firmware 3.3 or later, per public reporting. I could not confirm this from Danfoss itself.

Until you can update:

• Mitel: until the patch is applied, limit outside access to the MiCollab conferencing (AWV) component.

• Juniper: Juniper says there is no workaround, so upgrade.

• Xen Orchestra: if you can't update right away, take it off the internet and put it behind a VPN or management

network, as Vates advises.

- Danfoss: keep controllers off the public internet and on a separate, restricted network.

OFFICIAL SOURCES

CISA: CISA Adds 10 Known Exploited Vulnerabilities to Catalog (Nov 25, 2026) — https://www.cisa.gov/news-events/alerts/2026/11/25/cisa-adds-10-known-exploited-vulnerabilities-catalog
Mitel Product Security Advisory MISA-2026-0012 (MiCollab Multiple Vulnerabilities) — https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-misa-2026-0012
CISA ICS Advisory ICSA-25-140-03: Danfoss AK-SM 8xxA Series (Update A) — https://www.cisa.gov/news-events/ics-advisories/icsa-25-140-03

OTHER COVERAGE

SecurityWeek: Critical Juniper Session Smart Conductor Flaw Exploited in Attacks — https://www.securityweek.com/critical-juniper-session-smart-conductor-flaw-exploited-in-attacks/
eSecurityPlanet: Juniper Session Smart Conductor RCE Exploited, CISA Sets Nov. 28 Deadline — https://www.esecurityplanet.com/cybersecurity-threats/news-juniper-session-smart-conductor-cve-2026-103406-exploited/
BreachNews: Xen Orchestra Auth Bypass VSA-2026-062 Exploited in Attacks — https://breachnews.com/cyber-attacks/xen-orchestra-authentication-bypass-exploited-vsa-2026-062/
Ostorlab: Danfoss AK-SM 800A Auth Bypass Exploited (CVE-2025-41450) — https://blog.ostorlab.co/danfoss-ak-sm-800a-auth-bypass-cve-2025-41450.html

ABOUT THIS BRIEF

Last updated November 28, 2026. Researched with AI help from public sources and checked against the official advisories above. Details can change; follow your vendor's guidance.