contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

20 November 2026 · 3 new critical CVEs worth reading

Analysis Report

202 new records scored 8 or higher in the last 30 hours. 3 to read first, and the conditions each score leaves out.

PREPARED BY	NamiQ	DATE	20 November 2026
FACTS AS OF	20 November 2026	VERSION	1.0
TOP SCORE	Critical: 10.0	STATUS	Not on CISA's exploited list; exploitation not recorded

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/daily-cve-highlight-2026-11-20

The bottom line

> *Three unrelated products carry top-score flaws today: Mitel MiCollab and a D-Link router both let an attacker run commands, Mitel's without any login; a Flyto automation kernel lets files be written outside its sandbox. The sorting question: do you run any of these three?*

1522 CVE records were published in the last 30 hours. 202 scored 8 or higher. 3 are below, chosen by a fixed rule: highest score first, then fewest conditions in the wording, one product each. None is on CISA's exploited list, so a score here is the record's author describing the worst case. Read the condition before you act on the number.

At a glance

Product	Score	Fixed in	Read next
Mitel MiCollab (CVE-2026-133323)	10 (CVSS 3.1)	The vendor's advisory says a patch is available for release 10.3 (10.3.0.18) that addresses this flaw; upgrade to that release and apply the patch. No higher fixed build is named.	Technical Analysis
D-Link DIR-600L (CVE-2026-133493)	10 (CVSS 4.0)	See the note	Technical Analysis
flytohub flyto-core (CVE-2026-77312)	10 (CVSS 3.1)	flyto-core 2.26.8 (PyPI); the vendor's release notes call it a security release fixing this arbitrary file write and four other advisories.	Technical Analysis

Mitel MiCollab, CVE-2026-133323

If you run MiCollab, act now. Find whether the Audio, Web and Video Conferencing component is in use and on which version, then apply the vendor's patch for release 10.3 (10.3.0.18).

Score 10 (CVSS 3.1), published by Mitre on 19 November 2026. Weakness: CWE-78.

The record says an unauthenticated attacker who can reach the Audio, Web and Video Conferencing component of Mitel MiCollab can send crafted input the system then runs as commands. The limiting condition is being able to reach that component.

D-Link DIR-600L, CVE-2026-133493

If you run a DIR-600L on 2.17b02, treat it as exposed now. No fixed version is named, so restrict who can reach the device and plan a replacement.

Score 10 (CVSS 4.0), published by VulDB on 20 November 2026. Weakness: CWE-78, CWE-77.

The record says an attacker can send a crafted network request to the GENA handler of a D-Link DIR-600L router and make it run operating-system commands; no login is mentioned. It affects version 2.17b02, and reaching the device over the network is the only limit the record names.

flytohub flyto-core, CVE-2026-77312

If you run flyto-core, update to version 2.26.8 without delay. First list where it runs and which version each host has.

Score 10 (CVSS 3.1), published by GitHub on 19 November 2026. Weakness: CWE-22.

The record says someone able to run the product's modules or recipes can write files outside the intended sandbox folder of Flyto2 Core, because several data and file modules do not confine the output path. The limit is needing to run those modules or recipes.

Fifteen minutes this morning

- List the products above you run. If none, you are done.
- For each one you run, read the version from the product and compare it to the fixed version in the table.
- If it is in range, follow the note: reduce exposure first, then update.
- Book the update, and write down who owns it and by when.

Check your own project

If you build software, you can compare what a project declares with these CVEs from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE ids leave your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-133323,CVE-2026-133493,CVE-2026-77312
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same ids can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the hardware (maker, model, firmware), the running container images with their operating system and packages, and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on

it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-133323 --cve CVE-2026-133493 --cve CVE-2026-77312
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- These are new records. A record can change in the first days: scores, versions and wording are as at 20 November 2026. Nothing here has been tested.
- Exploitation is not recorded for any of them. That is not the same as none.
- The bottom line and the sentence under each product are our interpretation of the records and the vendors' pages, not a statement by the vendors.

Appendix 1. Severity decoded

CVE-2026-133323: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:H`

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Scope	Changed	Damage reaches beyond the vulnerable component.
Confidentiality	None	No data exposed.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

CVE-2026-133493: score 10, `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:P`

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Attack requirements	None	Works against a default deployment.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Vulnerable system: confidentiality	High	Total loss of confidentiality.
Vulnerable system: integrity	High	Total loss of integrity.
Vulnerable system: availability	High	Total loss of availability.
Subsequent systems: confidentiality	High	Total loss of confidentiality.
Subsequent systems: integrity	High	Total loss of integrity.
Subsequent systems: availability	High	Total loss of availability.

CVE-2026-77312: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:H`

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Scope	Changed	Damage reaches beyond the vulnerable component.
Confidentiality	None	No data exposed.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
19 November 2026	Mitel MiCollab, CVE-2026-133323: record published by Mitre.
20 November 2026	D-Link DIR-600L, CVE-2026-133493: record published by VulDB.
19 November 2026	flytohub flyto-core, CVE-2026-77312: record published by GitHub.

Appendix 3. Definition of done

- The products above you run are listed, with versions.
- Each in range has the vendor's fixed version and mitigation noted.
- The update is booked, with an owner and a date.
- Anything not in range is recorded as checked.

Sources

- CVE record service: https://www.cve.org/
- CVE record for CVE-2026-133323: https://www.cve.org/CVERecord?id=CVE-2026-133323
- CVE record for CVE-2026-133493: https://www.cve.org/CVERecord?id=CVE-2026-133493
- CVE record for CVE-2026-77312: https://www.cve.org/CVERecord?id=CVE-2026-77312