contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

10 November 2026 · 3 new critical CVEs worth reading

Analysis Report

444 new records scored 8.5 or higher in the last 30 hours. 3 to read first, and the conditions each score leaves out.

PREPARED BY	NamiQ	DATE	10 November 2026
FACTS AS OF	10 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-2026-11-10

The bottom line

> *All three records score 10; none require valid credentials to exploit: one sends a crafted SAML assertion to SAP NetWeaver, one intercepts cleartext credentials from a GeoVision GV-Face, one connects using a fixed MQTT credential baked into D-Link M60 firmware. Which of these three products do you run?*

2360 CVE records were published in the last 30 hours. 444 scored 8.5 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
SAP_SE SAP NetWeaver AS ABAP and ABAP Platform (SAML2 Service Provider) (CVE-2026-120017)	10 (CVSS 3.1)	See the note	Technical Analysis
GeoVision Inc. GV-Face (CVE-2026-124600)	10 (CVSS 4.0)	2.2.2 (the record names this as unaffected; no vendor advisory could be read to confirm a release date)	Technical Analysis
D-Link M60 (CVE-2026-125086)	10 (CVSS 4.0)	No unaffected or patched version is listed in the CVE record. The researcher's notes and the record name only firmware 1.12.B01; no source names a fixed release.	Technical Analysis

SAP_SE SAP NetWeaver AS ABAP and ABAP Platform (SAML2 Service Provider), CVE-2026-120017

If you run SAP NetWeaver AS ABAP with the SAML2 SP enabled, act without delay. The record does not name a patched version; restrict network access to the ABAP stack until SAP issues one.

Score 10 (CVSS 3.1), published by Sap on 10 November 2026. Weakness: CWE-347.

The record says SAP NetWeaver AS ABAP does not verify SAML assertions sufficiently in certain configurations. An unauthenticated attacker can impersonate any user, including administrators. The limiting condition is that the SAML2 SP must be active.

GeoVision Inc. GV-Face, CVE-2026-124600

Anyone running an affected version of GV-Face should update to 2.2.2, which the record names as unaffected. If the update cannot be applied at once, isolate the device from untrusted network segments.

Score 10 (CVSS 4.0), published by GV on 10 November 2026. Weakness: CWE-319.

The record says GV-Face sends user credentials over unencrypted HTTP. An attacker who can intercept traffic on the network path can read those credentials without logging in. The record names 2.2.2 as unaffected.

D-Link M60, CVE-2026-125086

No patched firmware is named in the record or any source read. Block untrusted access to TCP port 1883 at the VLAN or firewall boundary until D-Link issues a fix for firmware 1.12.B01.

Score 10 (CVSS 4.0), published by VulDB on 10 November 2026. Weakness: CWE-798, CWE-259.

The record says firmware 1.12.B01 contains a fixed MQTT credential; a researcher's notes add that the device restores it on every boot, so an admin password change does not remove it. Any device on the same network reaching TCP port 1883 can connect using it.

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-2026-120017,CVE-2026-124600,CVE-2026-125086
```

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-2026-120017 --cve CVE-2026-124600 --cve CVE-2026-125086
```

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 10 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-2026-120017: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/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	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

CVE-2026-124600: 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`

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-2026-125086: 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.

Appendix 2. Timeline

Date	Event
10 November 2026	SAP_SE SAP NetWeaver AS ABAP and ABAP Platform (SAML2 Service Provider), CVE-2026-120017: record published by Sap.
10 November 2026	GeoVision Inc. GV-Face, CVE-2026-124600: record published by GV.
10 November 2026	D-Link M60, CVE-2026-125086: record published by VulDB.

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-2026-120017: https://www.cve.org/CVERecord?id=CVE-2026-120017
- CVE record for CVE-2026-124600: https://www.cve.org/CVERecord?id=CVE-2026-124600
- CVE record for CVE-2026-125086: https://www.cve.org/CVERecord?id=CVE-2026-125086