contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

21 November 2026 · 3 new critical CVEs worth reading

Analysis Report

99 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	21 November 2026
FACTS AS OF	21 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-2026-11-21

The bottom line

> *All three records score 9.9 or above and each allows an attacker to take full control of the affected product. Two have no patch. The first question is whether any of these three products runs in your estate.*

615 CVE records were published in the last 30 hours. 99 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
Tegsoft Yönetim ve Bilişim Hizmetleri Tic. Ltd. Şti. Tegsoft Contact Center (CVE-2026-14914)	10 (CVSS 3.1)	The record states all versions before latest-202611161510 are affected, making that the first unaffected version. No vendor advisory was available to confirm this.	Technical Analysis
Danfoss AK-SC 355 (CVE-2026-127057)	9.9 (CVSS 4.0)	No fixed release. The record lists all versions as affected and names no unaffected release. The vendor says to migrate to the AK-SM800A series for ongoing security updates.	Technical Analysis
D-Link DCS-935L (CVE-2026-133680)	9.9 (CVSS 3.1)	See the note	Technical Analysis

Tegsoft Yönetim ve Bilişim Hizmetleri Tic. Ltd. Şti. Tegsoft Contact Center, CVE-2026-14914

Anyone running Tegsoft Contact Center should update to latest-202611161510 without delay. The record assigns a CVSS score of 10. No vendor advisory was available to confirm further detail.

Score 10 (CVSS 3.1), published by TR-CERT on 20 November 2026. Weakness: CWE-434.

The record says an attacker can upload a web shell to a Tegsoft Contact Center server and run commands on it. CWE-434 names this class of flaw. The record states no limiting condition.

Danfoss AK-SC 355, CVE-2026-127057

No patch exists for any version. Operators should change default credentials and remove public network exposure now, then plan migration to the AK-SM800A series as the vendor's record

recommends.

Score 9.9 (CVSS 4.0), published by Danfoss on 20 November 2026. Weakness: CWE-1392.

The record says an attacker who can reach a Danfoss AK-SC 355 or AK-SM 800 Series device over a network can log in using credentials that the vendor published in the product manual. The condition is that those credentials have not been changed.

D-Link DCS-935L, CVE-2026-133680

No fixed firmware is named in the sources. Any affected camera whose web interface is network-reachable should be isolated from untrusted paths or taken offline until a patch is available.

Score 9.9 (CVSS 3.1), published by VulDB on 20 November 2026. Weakness: CWE-78, CWE-77.

The record says an attacker who can reach the D-Link DCS-935L's web configuration interface can inject operating-system commands through the account or password fields in the local recording CGI. The VulDB record states the exploit has been made public.

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-2026-14914,CVE-2026-127057,CVE-2026-133680
```

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-2026-14914 --cve CVE-2026-127057 --cve CVE-2026-133680
```

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 21 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-2026-14914: 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-2026-127057: score 9.9, `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/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	Low	Some data exposed.
Subsequent systems: integrity	Low	Some data or behaviour can be altered.
Subsequent systems: availability	High	Total loss of availability.

CVE-2026-133680: score 9.9, `CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:X/RC:R`

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	Low	An ordinary account is enough.
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.

Appendix 2. Timeline

Date	Event
20 November 2026	Tegsoft Yönetim ve Bilişim Hizmetleri Tic. Ltd. Şti. Tegsoft Contact Center, CVE-2026-14914: record published by TR-CERT.
20 November 2026	Danfoss AK-SC 355, CVE-2026-127057: record published by Danfoss.
20 November 2026	D-Link DCS-935L, CVE-2026-133680: 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-2026-14914: https://www.cve.org/CVERecord?id=CVE-2026-14914
- CVE record for CVE-2026-127057: https://www.cve.org/CVERecord?id=CVE-2026-127057
- CVE record for CVE-2026-133680: https://www.cve.org/CVERecord?id=CVE-2026-133680