contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

1 November 2026 · 3 new critical CVEs worth reading

Analysis Report

23 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	1 November 2026
FACTS AS OF	1 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-2026-11-01

The bottom line

> *These are remote flaws in small network devices, and the records say exploits are public. The two WAVLINK flaws are command injection; the D-Link flaw is a stack-based buffer overflow. The sorting question: do you run one of these exact models or firmware versions?*

140 CVE records were published in the last 30 hours. 23 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
D-Link DIR-505 (CVE-2026-120189)	10 (CVSS 4.0)	See the note	Our note, below
WAVLINK WL-WN579A3-A (CVE-2026-120195)	10 (CVSS 4.0)	See the note	Our note, below
WAVLINK WL-WN530BE1-A (CVE-2026-120198)	10 (CVSS 4.0)	See the note	Our note, below

D-Link DIR-505, CVE-2026-120189

Act only if you run a DIR-505 on 1.10B02: cut outside access to it this week. No source we have names a fixed version, so ask D-Link what is available.

Score 10 (CVSS 4.0), published by VulDB on 1 November 2026. Weakness: CWE-121, CWE-119.

The record says the TFTP upload filename handler in D-Link DIR-505 1.10B02 has a stack-based buffer overflow that can be reached remotely. The record states no limiting condition.

WAVLINK WL-WN579A3-A, CVE-2026-120195

Act only if you run a WL-WN579A3-A: this week, check whether its admin pages can be reached from outside and close that. No fixed firmware is named, so ask your supplier.

Score 10 (CVSS 4.0), published by VulDB on 1 November 2026. Weakness: CWE-78, CWE-77.

The record says the wlan_ssid value in the setup wizard lets an attacker run operating system commands on a WAVLINK WL-WN579A3-A, remotely. The record states no limiting condition.

WAVLINK WL-WN530BE1-A, CVE-2026-120198

Act only if you run a WL-WN530BE1-A on V251117: this week, cut outside access to its web interface. No fixed firmware is named in our sources, so ask your supplier.

Score 10 (CVSS 4.0), published by VulDB on 1 November 2026. Weakness: CWE-77, CWE-74.

The record says the group_name or IP-FROM argument lets an attacker run commands on a WAVLINK WL-WN530BE1-A on V251117, remotely. The record states no limiting condition.

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.

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 1 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-2026-120189: 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-2026-120195: 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-2026-120198: 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
1 November 2026	D-Link DIR-505, CVE-2026-120189: record published by VulDB.
1 November 2026	WAVLINK WL-WN579A3-A, CVE-2026-120195: record published by VulDB.
1 November 2026	WAVLINK WL-WN530BE1-A, CVE-2026-120198: 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-2026-120189: https://www.cve.org/CVERecord?id=CVE-2026-120189
- CVE record for CVE-2026-120195: https://www.cve.org/CVERecord?id=CVE-2026-120195
- CVE record for CVE-2026-120198: https://www.cve.org/CVERecord?id=CVE-2026-120198