contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

3 November 2026 · 3 new critical CVEs worth reading

Analysis Report

101 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	3 November 2026
FACTS AS OF	3 November 2026	VERSION	1.0
TOP SCORE	Critical: 9.9	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-2026-11-03

The bottom line

> *All three records describe network-reachable flaws scored 9.8 or above, two with no stated login requirement. They involve TOTOLINK A950RG, SolarWinds Dameware, and Emerson Ovation. The question that sorts them: which is on your network, and is it reachable from outside?*

995 CVE records were published in the last 30 hours. 101 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
TOTOLINK A950RG (CVE-2026-121597)	9.9 (CVSS 3.1)	See the note	Our note, below
SolarWinds Dameware (CVE-2026-28336)	9.9 (CVSS 3.1)	SolarWinds Dameware 2026.3.1 (vendor advisory, published 3 November 2026)	Our note, below
Emerson Ovation (CVE-2022-29966)	9.8 (CVSS 3.1)	See the note	Our note, below

TOTOLINK A950RG, CVE-2026-121597

No fixed version is named in the record. If you use a TOTOLINK A950RG, block remote access to the management interface immediately and check with the vendor for a patch.

Score 9.9 (CVSS 3.1), published by VulDB on 4 November 2026. Weakness: CWE-121, CWE-119.

A stack-based buffer overflow in the TOTOLINK A950RG Easy Setup Wizard, triggered remotely via the functionType argument. An exploit is publicly available. Version 4.1.2cu.5268_B20221104 is named as affected. The record states no limiting condition.

SolarWinds Dameware, CVE-2026-28336

Upgrade SolarWinds Dameware to version 2026.3.1; the vendor's advisory, published 3 November 2026, names this as the fix. Until upgraded, block external access to Dameware.

Score 9.9 (CVSS 3.1), published by SolarWinds on 3 November 2026. Weakness: CWE-20.

A command injection flaw in SolarWinds Dameware that the vendor's advisory says could compromise the remotely controlled host. Authentication is required; the record indicates only low-level privileges suffice. Versions before 2026.3 are affected.

Emerson Ovation, CVE-2022-29966

No confirmed fixed version is named in the sources. Any site with Emerson Ovation should isolate it from untrusted networks now and contact Emerson for patch status.

Score 9.8 (CVSS 3.1), published by Icscert on 3 November 2026. Weakness: CWE-306.

Several protocols in Emerson Ovation carry no authentication. The record says an attacker who can reach the system over a network can change controller configuration or force a denial-of-service condition. 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.

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-2026-121597,CVE-2026-28336,CVE-2022-29966
```

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 names of running container images 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-2026-121597 --cve CVE-2026-28336 --cve CVE-2022-29966
```

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. It reads the names of the running images, not what is 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 3 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-2026-121597: 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.

CVE-2026-28336: score 9.9, `CVSS:3.1/AV:N/AC:L/PR:L/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	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.

CVE-2022-29966: score 9.8, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/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	Unchanged	Damage stays inside 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
4 November 2026	TOTOLINK A950RG, CVE-2026-121597: record published by VulDB.
3 November 2026	SolarWinds Dameware, CVE-2026-28336: record published by SolarWinds.
3 November 2026	Emerson Ovation, CVE-2022-29966: record published by Icscert.

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-2026-121597: https://www.cve.org/CVERecord?id=CVE-2026-121597
- CVE record for CVE-2026-28336: https://www.cve.org/CVERecord?id=CVE-2026-28336
- CVE record for CVE-2022-29966: https://www.cve.org/CVERecord?id=CVE-2022-29966