contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

# Daily CVE highlight

**3 November 2026 · 3 new critical CVEs worth reading**

## Analysis Report

74 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: 9.8 | 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 score 9.8 and require no administrator account to exploit. They cover unrelated products. The sorting question: is the specific condition present on your systems — an active WordPress add-on, an unpatched admin package, or a paired WSO2 configuration?*

491 CVE records were published in the last 30 hours. 74 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 |
|---|---|---|---|
| themefic Ultra Addons for Contact Form 7 (CVE-2026-102435) | 9.8 (CVSS 3.1) | No source in this record names a fixed version. The record describes all versions up to and including 3.5.54 as affected. | Our note, below |
| xianhc ape-volo-admin (CVE-2026-120442) | 9.8 (CVSS 3.1) | 3.6.1, released 31 October 2026 | Our note, below |
| WSO2 API Manager (CVE-2026-4052) | 9.8 (CVSS 3.1) | The record does not name a fixed version. No vendor advisory could be read at the time of writing. | Our note, below |

## themefic Ultra Addons for Contact Form 7, CVE-2026-102435

Disable the PDF Generator add-on now if it is active. No source names a fixed version; there is no patch yet. If this plugin is not installed, no action needed.

Score 9.8 (CVSS 3.1), published by Wordfence on 2 November 2026. Weakness: CWE-502.

An unauthenticated visitor can delete any file on the server, which the record says can lead to remote code execution. Affects Ultra Addons for Contact Form 7 up to version 3.5.54. The PDF Generator add-on must be active for the flaw to be reachable.

## xianhc ape-volo-admin, CVE-2026-120442

Update to 3.6.1, released 31 October 2026. Any instance before that version is open to token forgery with no network requirement. If you do not run ape-volo-admin, no action needed.

Score 9.8 (CVSS 3.1), published by VulnCheck on 2 November 2026. Weakness: CWE-1394.

An attacker can forge an administrator token offline using a signing key the record says is hardcoded in the configuration file. With that token they gain full API control over users, roles, permissions and data. Affects ape-volo-admin before 3.6.1.

## WSO2 API Manager, CVE-2026-4052

Check whether Identity Server is your Resident Key Manager with shared databases. If so and you run 4.1.0–4.4.0, treat this as active: no source names a fix. Otherwise this CVE does not apply.

Score 9.8 (CVSS 3.1), published by WSO2 on 3 November 2026. Weakness: CWE-862.

A self-registered user can reach the System REST APIs of WSO2 API Manager via a token from the Identity Server endpoint. Affects versions 4.1.0–4.4.0. The record says this only applies where Identity Server is the Resident Key Manager with shared databases.

## 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-2026-102435,CVE-2026-120442,CVE-2026-4052
```

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-2026-102435 --cve CVE-2026-120442 --cve CVE-2026-4052
```

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-2026-102435**: 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. |

**CVE-2026-120442**: 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. |

**CVE-2026-4052**: 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 |
|---|---|
| 2 November 2026 | themefic Ultra Addons for Contact Form 7, CVE-2026-102435: record published by Wordfence. |
| 2 November 2026 | xianhc ape-volo-admin, CVE-2026-120442: record published by VulnCheck. |
| 3 November 2026 | WSO2 API Manager, CVE-2026-4052: record published by WSO2. |

## 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-2026-102435: https://www.cve.org/CVERecord?id=CVE-2026-102435
- CVE record for CVE-2026-120442: https://www.cve.org/CVERecord?id=CVE-2026-120442
- CVE record for CVE-2026-4052: https://www.cve.org/CVERecord?id=CVE-2026-4052