contact@namiq.io · namiq.io

NamiQ

DAILY CVE HIGHLIGHT

Daily CVE highlight

18 November 2026 · 3 new critical CVEs worth reading

Analysis Report

340 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	18 November 2026
FACTS AS OF	18 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-2026-11-18

The bottom line

> *All three new records score 10 and let a remote attacker take control without a valid login. One question sorts them: do you run Rucio, ASUS Control Center Express or Oracle Business Intelligence Enterprise Edition, and can anyone outside your control reach it?*

1685 CVE records were published in the last 30 hours. 340 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
rucio (CVE-2026-100397)	10 (CVSS 3.1)	35.9.1, 38.6.1, 40.4.2, 41.1.1 (as the CVE record states them)	Technical Analysis
ASUS Control Center Express (CVE-2026-114202)	10 (CVSS 4.0)	See the note	Technical Analysis
Oracle Corporation Oracle Business Intelligence Enterprise Edition (CVE-2026-114784)	10 (CVSS 3.1)	See the note	Technical Analysis

rucio, CVE-2026-100397

Rucio users: upgrade to 35.9.1, 38.6.1, 40.4.2 or 41.1.1 this week, starting with any server reachable from untrusted networks. Everyone else can ignore it.

Score 10 (CVSS 3.1), published by GitHub on 17 November 2026. Weakness: CWE-287.

The record says an attacker with no login can name any account, including an administrative one, get a short-lived SSH challenge token and use it as a login token. The record states no limiting condition.

ASUS Control Center Express, CVE-2026-114202

If you run it, find the installed version this week and ask ASUS for the fixed release. The record names no fixed version. Everyone else can ignore it.

Score 10 (CVSS 4.0), published by ASUS on 18 November 2026. Weakness: CWE-321.

The record says a hard-coded cryptographic key lets a remote user forge an authentication token and gain administrative privileges in this management product. The record states no limiting

condition.

Oracle Corporation Oracle Business Intelligence Enterprise Edition, CVE-2026-114784

If you run it, check today whether it can be reached over HTTP. The record names no fixed version, so ask Oracle which update applies. Everyone else can ignore it.

Score 10 (CVSS 3.1), published by Oracle on 17 November 2026. Weakness: Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. While the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Business Intelligence Enterprise Edition..

The record says an attacker with no login can take over this Oracle reporting platform, and other products may be affected. The limiting condition is that the attacker needs network access over HTTP.

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-2026-100397,CVE-2026-114202,CVE-2026-114784
```

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-2026-100397 --cve CVE-2026-114202 --cve CVE-2026-114784
```

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 18 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-2026-100397: 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-2026-114202: 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-2026-114784: 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.

Appendix 2. Timeline

Date	Event
17 November 2026	rucio, CVE-2026-100397: record published by GitHub.
18 November 2026	ASUS Control Center Express, CVE-2026-114202: record published by ASUS.
17 November 2026	Oracle Corporation Oracle Business Intelligence Enterprise Edition, CVE-2026-114784: record published by Oracle.

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-2026-100397: https://www.cve.org/CVERecord?id=CVE-2026-100397
- CVE record for CVE-2026-114202: https://www.cve.org/CVERecord?id=CVE-2026-114202
- CVE record for CVE-2026-114784: https://www.cve.org/CVERecord?id=CVE-2026-114784