contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Oracle Corporation Oracle Business Intelligence Enterprise Edition: new CVE

CVE-2026-114784 · record published 17 November 2026

Analysis Report

Anyone running Oracle Business Intelligence Enterprise Edition 8.2.0.0.0 or 26.01.0.0.0 should treat this as urgent, starting today, 17 November 2026. First find

PREPARED BY	NamiQ	DATE	17 November 2026
FACTS AS OF	17 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 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/oracle-corporation-oracle-business-cve-2026-114784

The bottom line

> *Anyone running Oracle Business Intelligence Enterprise Edition 8.2.0.0.0 or 26.01.0.0.0 should treat this as urgent, starting today, 17 November 2026. First find out whether it is run and whether it can be reached over HTTP. If you do not run it, stop reading.*

At a glance

Fact	Detail
Product	Oracle Corporation Oracle Business Intelligence Enterprise Edition (CVE-2026-114784)
Severity	Critical: 10 (CVSS 3.1)
Status	A new CVE record, published by Oracle on 17 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 17 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	No source we read names a fixed version
Who looks first	Firms and IT providers running Oracle Business Intelligence Enterprise Edition (part of Oracle Analytics) at version 8.2.0.0.0 or 26.01.0.0.0, especially where the web interface can be reached from outside.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Oracle Business Intelligence Enterprise Edition (Oracle Analytics)?	Nothing to do for this CVE.	Check the version (next question).
Is the version 8.2.0.0.0 or 26.01.0.0.0?	Ask Oracle or your provider whether your version is affected.	Check who can reach it over HTTP.
Can anyone outside your trusted network reach it over HTTP?	Lower urgency, but still plan the fix.	Restrict access now and ask for the fix.
Does it sit beside other Oracle or business systems?	Impact is limited to this server.	The record says other products may be affected; include them in the review.

What it is

The record says an attacker with no login and only network access over HTTP can take over Oracle Business Intelligence Enterprise Edition. It rates the attack as easy, and says other products may be affected too.

Why it matters

Our reading is that a score of 10 with no login, no user action and a scope change makes this a priority even though CISA does not list it. A takeover of a reporting platform would typically give access to the data it reads and to systems connected to it. The record names no fixed version.

Things people will get wrong

- "It is not on CISA's list, so it is safe to wait." The record is new. A missing listing does not show that nobody is exploiting it, and the record rates it easy to exploit without a login.
- "It only affects the Business Intelligence server." The record says a scope change means attacks may significantly impact additional products.
- "A firewall in front of it is enough." The record says the attack comes over HTTP, so any path to the web interface counts. Check who can reach it.

How we would triage it

This is our judgement.

Step 1: Find the versions you run

- Ask who runs Oracle Business Intelligence Enterprise Edition and on which hosts.
- Note the exact version. The record lists 8.2.0.0.0 and 26.01.0.0.0 as affected.

Step 2: Reduce exposure

- Limit HTTP access to the product to people who need it, until a fix is confirmed.
- Remove any route to it from the internet where you can.

Step 3: Ask Oracle for the fix

- No source we read names a fixed version, so ask Oracle or your provider which update applies.
- Apply it as soon as it is confirmed and tested.

Step 4: Check for signs of misuse

- Review web access logs for unusual requests to the product from unknown addresses.
- Check for new accounts or changed settings on the product.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *Hello, we need to know whether we run Oracle Business Intelligence Enterprise Edition (Oracle Analytics), and if so which version and where. The record for CVE-2026-114784 lists versions 8.2.0.0.0 and 26.01.0.0.0 as affected, and it rates the flaw 10.0. Please tell us whether it can be reached over HTTP from outside, restrict access if so, and name the fixed version. Please confirm the version and the fix in writing by 24 November 2026.*

The weakness behind it

The listing classes this as 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..

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so
Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page.	Initial Access: getting in	The record describes an unauthenticated attack over HTTP on a network-facing component, so it would likely be used to gain first access through the exposed web service.

Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	A takeover with full integrity impact would typically allow an attacker to run commands on the system, though the record does not say how.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

The CVE record:

> *Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Platform Security). Supported versions that are affected are 8.2.0.0.0 and 26.01.0.0.0. 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. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). ...*

Versions of Oracle Corporation Oracle Business Intelligence Enterprise Edition the record lists as affected:

- 8.2.0.0.0
- 26.01.0.0.0

The record gives no version ranges. Use the vendor's advisory for the affected versions.

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve 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 id 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-2026-114784
```

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

- Which version fixes it. The record does not name one and no vendor page could be read.
- Whether anyone is exploiting it. CISA does not list it, which does not rule it out.
- Which other products the scope change reaches.
- Whether a workaround exists.
- Exploitation is not recorded. That is not the same as none.
- This is a new record: scores, versions and wording can change in the first days, and they are as at 17 November 2026. We have not read the vendor's advisory page and we have not tested it.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "Likely ATT&CK mapping", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-114784: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H` As the CVE record gives it.

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	CVE record published by Oracle.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
Affected version, reachable from the internet	High	Today; restrict access first
Affected version, reachable only from the internal network	Medium	This week
Affected version, access limited to a small trusted group	Medium	Within the next patch cycle
Version not listed in the record	Low	Confirm with your provider
Product not in use	None	None for this CVE

Appendix 4. Definition of done

- Every Oracle Corporation Oracle Business Intelligence Enterprise Edition you run is listed, with its version.
- Each is outside the affected list, or the vendor's fix or mitigation is in place.
- The version output or a screenshot is saved with the date.
- Anything not done has an owner and a date.

Sources

- CVE record for CVE-2026-114784: https://www.cve.org/CVERecord?id=CVE-2026-114784
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Reference in the CVE record: www.oracle.com: https://www.oracle.com/security-alerts/cspunov2026.html