contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

SAP NetWeaver exploited

CVE-2025-42884 · on CISA's exploited list since 20 November 2026

Analysis Report

Organisations running SAP NetWeaver Enterprise Portal on EP-BASIS 7.50 or EP-RUNTIME 7.50 must act; CISA's deadline of 23 November 2026 has already passed. Apply SAP Security Note 3660969 immediately ...

PREPARED BY	NamiQ	DATE	24 November 2026
FACTS AS OF	24 November 2026	VERSION	1.0
SEVERITY	**Medium: CVSS 3.1 6.5**	STATUS	On CISA's exploited list; due 23 November 2026

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/sap-netweaver-cve-2025-42884

The bottom line

> *Organisations running SAP NetWeaver Enterprise Portal on EP-BASIS 7.50 or EP-RUNTIME 7.50 must act; CISA's deadline of 23 November 2026 has already passed. Apply SAP Security Note 3660969 immediately — no authentication is needed to attempt the attack.*

At a glance

Fact	Detail
Product	SAP NetWeaver (CVE-2025-42884)
Severity	Medium: 6.5 (CVSS 3.1)
CISA	On its exploited list since 20 November 2026. Deadline for US federal agencies: 23 November 2026.
Chance of exploitation (EPSS)	0.01, the estimated chance in the next 30 days, as at 24 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	No specific patched version number is named in the sources. The vendor's advisory lists SAP Security Note 3660969 as the correction for EP-BASIS 7.50 and EP-RUNTIME 7.50.
Who looks first	Anyone responsible for SAP NetWeaver Enterprise Portal where EP-BASIS 7.50 or EP-RUNTIME 7.50 is installed. No login is required, so any network path that reaches the portal is sufficient to attempt the attack.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run SAP NetWeaver Enterprise Portal?	Nothing to do for this CVE.	Check which component versions are installed.
Are you running EP-BASIS 7.50 or EP-RUNTIME 7.50?	Not in scope per the record; no action needed.	Apply SAP Security Note 3660969.
Can unauthenticated users reach the portal from outside your network?	Lower immediate risk, but still apply the note at your next change window.	Treat as urgent; apply the note or restrict access immediately.

What it is

An unauthenticated attacker can inject JNDI environment properties or supply a URL for the portal's JNDI lookup operations, redirecting them to an unintended JNDI provider. The record says this can lead to disclosure or modification of information about the server. The record states there is no impact on availability.

Why it matters

The record scores this 6.5, but no authentication is required and the flaw is reachable over a network. The attacker gains access to an unintended JNDI provider, which the record says can lead to server information being disclosed or modified. Our reading is that the low bar to attempt the attack — network-reachable and requiring no credentials — matters more here than the numeric score alone. Organisations with the portal exposed to the internet face the greatest practical risk.

What the vendor's advisory says

We read two pages on support.sap.com. In short:

- The November 2025 SAP Patch Day included CVE-2025-42944 (Critical, CVSS 10.0): insecure deserialisation in SAP NetWeaver AS Java (SERVERCORE 7.50), SAP Note 3660659, listed as an update to the October 2025 patch.
- CVE-2025-42887 (Critical, CVSS 9.9): code injection in SAP Solution Manager (ST 720), SAP Note 3668705.
- CVE-2025-42940 (High, CVSS 7.5): memory corruption in SAP CommonCryptoLib (CRYPTOLIB 8), SAP Note 3633049.
- CVE-2025-42882 (Medium, CVSS 4.3): missing authorisation check in SAP NetWeaver AS for ABAP (SAP_BASIS versions 700 through 816), SAP Note 3643337.

Things people will get wrong

- A CVSS score of 6.5 means this can wait for the next regular patch cycle. No authentication is required; anyone who can reach the portal can attempt the attack. The vendor's advisory lists the correction as a priority, and CISA listed this as known exploited.
- No availability impact means attackers cannot do real damage here. The record also states modification of server information is possible. The attacker gains access to an unintended JNDI provider, which is a capability beyond reading a file.

How we would triage it

This is our judgement.

Step 1: Find which portal component versions are installed

- Check whether EP-BASIS 7.50 or EP-RUNTIME 7.50 is present in your landscape; these are the only versions the record names as affected.
- Your SAP administrator can confirm installed component versions via the SAP Management Console or SAP NetWeaver Administrator.

Step 2: Restrict portal access if patching must be delayed

- If the portal is reachable from outside your network and the note cannot be applied immediately, restrict access to trusted network addresses as an interim measure.
- The record states no authentication is required; limiting who can reach the portal is the most direct interim control.

Step 3: Apply SAP Security Note 3660969

- The vendor's advisory lists SAP Security Note 3660969 as the correction for EP-BASIS 7.50 and EP-RUNTIME 7.50; follow the vendor's implementation instructions.
- No specific patched version number is named in the sources; ask your SAP administrator to confirm the note has been applied and any required system restart has completed.

Step 4: Check for signs of earlier exploitation

- Review portal access logs for requests containing JNDI-pattern strings in URL parameters or HTTP headers targeting portal endpoints.
- Look for unexpected outbound connections from the portal server to LDAP, RMI, or other JNDI-capable services, which may indicate a lookup was redirected to an attacker-controlled provider.

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. CISA's wording adds that you should stop using the product if no mitigation is available.

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.

> *We are following up on CVE-2025-42884, a JNDI injection vulnerability in SAP NetWeaver Enterprise Portal. The record identifies EP-BASIS 7.50 and EP-RUNTIME 7.50 as affected versions. CISA's remediation deadline of 23 November 2026 has already passed. Please confirm whether we run SAP NetWeaver Enterprise Portal and, if so, which versions of EP-BASIS and EP-RUNTIME are installed. If either affected version is present, please apply SAP Security Note 3660969 per the vendor's instructions and provide written confirmation of the installed version and the fix applied by 27 November 2026.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Portal access logs showing requests with JNDI-pattern strings in URL parameters or HTTP headers targeting portal components, which may indicate injection attempts.
- Outbound network connections from the portal server to unexpected LDAP, RMI, or other JNDI-capable services, which may indicate a successful lookup redirection to an external provider.

The weakness behind it

The record classes this as CWE-943 (Improper Neutralization of Special Elements in Data Query Logic).

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 flaw is network-reachable with no authentication required, targeting a public-facing enterprise portal. This would typically be the initial access technique for a remote attacker.
System Information Discovery (T1082): Reading the details of a system, such as its version and configuration.	Discovery: looking around	The record states the attack can lead to disclosure of server information, which would likely involve reading configuration or environment details accessible via the unintended JNDI provider.
Data Manipulation: Stored Data Manipulation (T1565.001): Changing stored data without permission.	Impact: causing damage or disruption	The record states modification of server information is also possible, which would typically map to manipulation of data stored on the server via the JNDI injection path.

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

CISA's catalogue entry:

> *SAP NetWeaver Enterprise Portal contains an improper neutralization of special elements in data query logic vulnerability that allows an unauthenticated attacker to disclose or modify server information via injected JNDI environment properties or a URL used during JNDI lookup operations.*

The CVE record, published by Sap on 11 November 2025:

> *SAP NetWeaver Enterprise Portal allows an unauthenticated attacker to inject JNDI environment properties or pass a URL used during JNDI lookup operations, enabling access to an unintended JNDI provider.This could further lead to disclosure or modification of information about the server. There is no impact on availability.*

Versions of SAP_SE SAP NetWeaver Enterprise Portal the record lists as affected:

- EP-BASIS 7.50
- EP-RUNTIME 7.50

CISA's required action:

> *Apply mitigations in accordance with vendor instructions.*

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-2025-42884
```

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-2025-42884
```

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

- The sources do not identify which specific portal endpoints or request parameters are injectable.
- The sources do not state whether a workaround — such as disabling a portal component — exists as an alternative to applying the note.
- The record does not describe what further capability an attacker gains from access to an unintended JNDI provider beyond information disclosure and modification.
- No specific patched version number is named in the sources; the correction is referenced only by SAP Security Note number 3660969.

- We have not tested this against any environment. Versions and scores are as the sources state them and as at 24 November 2026; the vendor's advisory wins where it differs.
- 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-2025-42884: score 6.5, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

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	Low	Some data exposed.
Integrity	Low	Some data or behaviour can be altered.
Availability	None	No effect on availability.

Appendix 2. Timeline

Date	Event
11 November 2025	CVE record published by Sap.
20 November 2026	CISA added it to its list of exploited vulnerabilities.
23 November 2026	CISA's deadline for US federal agencies.

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
SAP NetWeaver Enterprise Portal on EP-BASIS 7.50 or EP-RUNTIME 7.50, reachable from outside the network	High	Immediately — CISA deadline of 23 November 2026 has passed
SAP NetWeaver Enterprise Portal on EP-BASIS 7.50 or EP-RUNTIME 7.50, internal network only	High	Within this patch cycle
SAP NetWeaver Enterprise Portal on affected version; patch cannot be applied yet	Medium	Restrict portal network access as an interim measure now

Running SAP NetWeaver AS Java on SERVERCORE 7.50 alongside the portal	High	Same patch batch includes CVE-2025-42944 at CVSS 10.0

Appendix 4. Definition of done

- Every SAP NetWeaver you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Your projects' declared dependencies were checked against this CVE, and every row has a written reason.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2025-42884: https://www.cve.org/CVERecord?id=CVE-2025-42884
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: support.sap.com/en/my-support/knowledge-base/security-notes-new: https://support.sap.com/en/my-support/knowledge-base/security-notes-news.html?anchorId=section_370125364
- Advisory or release notes read: support.sap.com/en/my-support/knowledge-base/security-notes-new: https://support.sap.com/en/my-support/knowledge-base/security-notes-news/bulletin-2025.html
- Reference in the CVE record: me.sap.com: https://me.sap.com/notes/3660969
- Reference in the CVE record: url.sap: https://url.sap/sapsecuritypatchday