CISA flags SAP NetWeaver Enterprise Portal flaw CVE-2025-42884



CISA lists CVE-2025-42884, a flaw in SAP NetWeaver Enterprise Portal that lets an unauthenticated attacker disclose or modify server information through JNDI lookup manipulation. Mitigate per SAP's instructions.

- CVE-2025-42884 affects SAP NetWeaver Enterprise Portal.
- The cause is improper neutralization of special elements in data query logic.
- An unauthenticated attacker can disclose or modify server information.
- The attack uses injected JNDI environment properties or a URL in JNDI lookups.
- CISA's federal due date is 2026-11-23, and it refers to its BOD 26-04 guidance and forensics triage requirements.

What was reported

CISA has listed CVE-2025-42884, a vulnerability in the SAP NetWeaver Enterprise Portal. The flaw is described as improper neutralization of special elements in data query logic. An unauthenticated attacker can use it to disclose or modify information on the server.

The technique involves injecting JNDI environment properties, or supplying a URL that is used during a JNDI lookup operation. Because no authentication is needed, any instance reachable by an attacker deserves attention.

What CISA asks for

CISA's required action is to apply mitigations following the vendor's instructions, in line with its BOD 26-04 guidance on prioritizing security updates based on risk, and its Forensics Triage Requirements. Where mitigations are not available, the guidance is to follow the applicable BOD 26-04 provisions for cloud services or stop using the product. Stakeholders are responsible for assessing the internet exposure of each asset. The federal due date is 2026-11-23.

The source does not give affected version numbers or details of exploitation, so SAP's own advisory should be the reference for those.

Practical view for Saudi institutions

The due date applies to US federal bodies, but the risk logic carries over to any organization running Enterprise Portal. Start by establishing where the portal is deployed and whether it is exposed to the internet, then apply SAP's mitigations and keep evidence of the work for audit purposes.

What to do now

1. Inventory all SAP NetWeaver Enterprise Portal instances and record which are reachable from the internet.
2. Apply SAP's published mitigations for CVE-2025-42884 and record the change.
3. Prioritize internet-facing instances and, where practical, restrict access until mitigation is complete.
4. Review portal and server logs for unusual JNDI-related requests and preserve evidence if anything is found.
5. Raise the item in vulnerability management and report status to the CISO under NCA ECC and SAMA CSF processes.