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



CISA lists CVE-2025-42884, an injection flaw in SAP NetWeaver Enterprise Portal that lets an unauthenticated attacker read or alter server information through JNDI lookups. Apply vendor mitigations and review internet exposure.

- The flaw affects SAP NetWeaver Enterprise Portal and is an improper neutralization of special elements in data query logic.
- An unauthenticated attacker can disclose or modify server information.
- The attack works through injected JNDI environment properties or a URL used in JNDI lookup operations.
- CISA requires vendor mitigations, BOD 26-04 compliance and its forensics triage requirements; the federal due date is 2026-11-23.

> - Where mitigations are unavailable, CISA says to stop using the product.

CISA has added CVE-2025-42884 to its list of vulnerabilities, describing an improper neutralization of special elements in the data query logic of SAP NetWeaver Enterprise Portal.

What the flaw allows

An unauthenticated attacker can disclose or modify information held on the server. The route is the injection of JNDI environment properties, or of a URL used during a JNDI lookup operation. No credentials are needed, which makes any reachable Enterprise Portal instance a point of concern.

What CISA asks for

CISA directs organisations to apply mitigations according to the vendor's instructions, in line with its BOD 26-04 guidance on prioritizing security updates based on risk, and with its Forensics Triage Requirements. For cloud services, the applicable BOD 26-04 guidance should be followed. If mitigations are not available, CISA says use of the product should be discontinued. Stakeholders are responsible for assessing the internet exposure of each asset and following the patching timelines. The federal due date is 2026-11-23.

Practical reading for Saudi institutions

The directive is aimed at US federal bodies, but the technical risk is the same for any organisation running SAP NetWeaver Enterprise Portal. The source does not name affected versions or patch numbers, so teams should rely on SAP's own advisory for those details. Start by establishing where the portal runs and whether it can be reached from the internet, then apply the vendor's mitigations and check for signs of misuse.

What to do now

1. Inventory all SAP NetWeaver Enterprise Portal instances and record which are reachable from the internet.
2. Apply the mitigations in SAP's instructions, prioritising internet-facing instances.
3. Where mitigations are not available, plan to restrict access or retire the component, as CISA advises.
4. Review portal and server logs for unusual JNDI lookups or unexpected outbound URL requests.
5. Record the exposure assessment and remediation under your vulnerability management process and report to the CISO.