SAP fixes four maximum-severity flaws in NetWeaver and Web Dispatcher



SAP's monthly Patch Day fixed four flaws rated CVSS 10.0 that can be exploited without logging in. Three affect SAP NetWeaver application server and one affects the Web Dispatcher.

- Four flaws were fixed in SAP's monthly Security Patch Day, each rated 10.0, the maximum CVSS score.
- Attackers could exploit all four without authentication.
- Three flaws are in SAP NetWeaver application server, the software SAP systems run on.
- One flaw is in the Web Dispatcher, which receives internet web requests and forwards them to the application server.
- The headline states that two of the flaws enable remote code execution.

SAP released its monthly Security Patch Day updates and fixed four vulnerabilities that the vendor scores at 10.0, the highest possible CVSS rating. According to the report, attackers could exploit all four without logging in.

What is affected

Three of the flaws are in SAP NetWeaver application server, the software on which SAP systems run. The fourth is in the Web Dispatcher, the component that receives web requests from the internet and passes them to that server. The report's headline notes that two of the four allow remote code execution.

The excerpt available to us does not give CVE identifiers, affected versions or any evidence of exploitation, so those details should be taken from SAP's official security notes.

Why it matters

Because the flaws require no authentication, and the Web Dispatcher sits at the point where internet traffic reaches SAP landscapes, systems exposed to the internet carry the greatest risk. Organisations that run SAP for finance, procurement or HR should treat this release as a priority and not wait for the usual patch cycle.

What to do next

Confirm which NetWeaver and Web Dispatcher instances you run, review SAP's notes for the affected versions, and schedule the fixes through your emergency change process, beginning with internet-facing systems.

What to do now

1. Inventory all SAP NetWeaver application server and Web Dispatcher instances, noting which are reachable from the internet.
2. Review SAP's official security notes for this Patch Day to identify affected versions and the corrections for the four CVSS 10.0 flaws.
3. Apply the patches through an emergency change process, starting with internet-facing systems.
4. Where patching cannot happen immediately, restrict access to Web Dispatcher and monitor it closely for unusual requests.
5. Record the assessment and remediation to evidence vulnerability management under NCA ECC and SAMA CSF.