

NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-44758

Summary

CVE-2026-44758 is a newly disclosed Critical vulnerability. It is not yet on CISA's actively-exploited list; treat it as proactive patching before it is weaponised. SAP Manufacturing Integration and Intelligence (MII) allows an attacker with high privileges to submit specially crafted input to certain affected functionality, which is processed without sufficient validation. Successful exploitation could allow the attacker to execute arbitrary commands on the underlying operating system, resulting in high impact on confidentiality, integrity, and availability of the application.

What we know

- **CVE:** CVE-2026-44758
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 9.1 Critical, Network-exploitable, no user interaction (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H)

Recommended action

Patch as a fix becomes available, prioritised by the exposure and EPSS above. Until then, limit network exposure of the affected service and tighten access until patched. This does not yet trigger CRA 24-hour reporting, which requires active exploitation, but patching ahead of exploitation is the whole point.

Sources: NIST NVD. Public data; an advisory of a newly disclosed vulnerability, not an incident report. Verify applicability to your estate before acting.