

CVE-2017-12637

SAP NetWeaver Directory Traversal Vulnerability

CISA KEV since Mar 19, 2025

Actively exploited

Directory traversal vulnerability in scheduler/ui/js/fffffffbca41eb4/UIUtilJavaScriptJS in SAP NetWeaver Application Server Java 7.5 allows remote attackers to read arbitrary files via a .. (dot dot) in the query string, as exploited in the wild in August 2017, aka SAP Security Note 2486657.

EVRS 84/100 Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.951 99.87th percentile · FIRST	CISA DEADLINE Apr 9, 2025 KEV since 2025 · listed over a year
--	--	---	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.951 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
netweaver application server java	7.50	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-5p56-56jf-wfv2	SAP users must have an account to log in and access the patch	me.sap.com/notes/3476549
NVD	nvd.nist.gov/vuln/detail/CVE-2017-12637	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2017-4176	Current data	evulnable.com/vulnerability-management/cve/CVE-2017-12637

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.