

CVE-2016-2388

SAP NetWeaver Information Disclosure Vulnerability

CISA KEV since Jun 9, 2022

Actively exploited

The Universal Worklist Configuration in SAP NetWeaver AS JAVA 7.4 allows remote attackers to obtain sensitive user information via a crafted HTTP request, aka SAP Security Note 2256846.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 5.3 Medium · NVD	EPSS 0.522 99th percentile · FIRST	CISA DEADLINE Jun 30, 2022 KEV since 2022 · 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	On the CISA KEV catalog for over two years
☒ EPSS	0.522 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 5.3	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle No patch reported by the connected remediation source

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
netweaver application server java	≥ 7.10 ≤ 7.50	after 7.50	NVD

Sources

Vendor guidance erpscan.io/advisories/erpscan-16-010-sap-netweaver-7-4-information-disclosure/
NVD nvd.nist.gov/vuln/detail/CVE-2016-2388

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2016-3472

Additional guidance erpscan.io/press-center/blog/sap-security-notes-february-2016-review/

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

Current data evulnable.com/vulnerability-management/cve/CVE-2016-2388

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