

CVE-2016-2386

SAP NetWeaver SQL Injection Vulnerability

CISA KEV since Jun 9, 2022

Actively exploited

SQL injection vulnerability in the UDDI server in SAP NetWeaver J2EE Engine 7.40 allows remote attackers to execute arbitrary SQL commands via unspecified vectors, aka SAP Security Note 2101079.

EVRS 79 / ₁₀₀ Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.715 99.42nd 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	0.715 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

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	7.40	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-g384-79gw-fw4	NVD	nvd.nist.gov/vuln/detail/CVE-2016-2386
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2016-3470
Current data	evulnable.com/vulnerability-management/cve/CVE-2016-2386		

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