

CVE-2019-0344

SAP Commerce Cloud Deserialization of Untrusted Data Vulnerability

CISA KEV since Sep 30, 2024

Actively exploited

Due to unsafe deserialization used in SAP Commerce Cloud (virtualjdbc extension), versions 6.4, 6.5, 6.6, 6.7, 1808, 1811, 1905, it is possible to execute arbitrary code on a target machine with 'Hybris' user rights, resulting in Code Injection.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.071 94.2nd percentile · FIRST	CISA DEADLINE Oct 21, 2024 KEV since 2024 · 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	0.071 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 mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
commerce cloud	6.4 6.5 6.6 6.7 1808 1811 1905	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-75jg-chc9-wv8p	Additional guidance	launchpad.support.sap.com/#/notes/2786035
web.archive.org	web.archive.org/web/20191214053020/https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=523998017	NVD	nvd.nist.gov/vuln/detail/CVE-2019-0344
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2019-1117
Current data	evulnable.com/vulnerability-management/cve/CVE-2019-0344		

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