

CVE-2024-40711

Veeam Backup and Replication Deserialization Vulnerability

Exigent

CISA KEV since Oct 17, 2024

Actively exploited

Ransomware use known

A deserialization of untrusted data vulnerability with a malicious payload can allow an unauthenticated remote code execution (RCE).

EVRS 91/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.904 99.8th percentile · FIRST	CISA DEADLINE Nov 7, 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.904 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent 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
veeam backup \& replication	≥ 12.0.0.1420 < 12.2.0.334	12.2.0.334	NVD

Sources

Vendor guidance github.com/advisories/GHSA-c76v-gjqc-j462
NVD nvd.nist.gov/vuln/detail/CVE-2024-40711

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2024-38578

Additional guidance veeam.com/kb4649

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

Current data evulnable.com/vulnerability-management/cve/CVE-2024-40711

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