

CVE-2023-27532

Veeam Backup & Replication Cloud Connect Missing Authentication for Critical Function Vulnerability

CISA KEV since Aug 22, 2023

Actively exploited

Ransomware use known

Vulnerability in Veeam Backup & Replication component allows encrypted credentials stored in the configuration database to be obtained. This may lead to gaining access to the backup infrastructure hosts.

EVRS 85/100 Immediate priority	CVSS V3.1 7.5 High · NVD	EPSS 0.806 99.63rd percentile · FIRST	CISA DEADLINE Sep 12, 2023 KEV since 2023 · 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	0.806 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately 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	< 11.0.1.1261 11.0.1.1261 12.0.0.1420	11.0.1.1261	NVD

Sources

Vendor guidance github.com/advisories/GHSA-hh3c-xpmg-w5fr
NVD nvd.nist.gov/vuln/detail/CVE-2023-27532

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2023-31287

Additional guidance veeam.com/kb4424

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

Current data evulnable.com/vulnerability-management/cve/CVE-2023-27532

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