

CVE-2023-34048

VMware vCenter Server Out-of-Bounds Write Vulnerability

Exigent

CISA KEV since Jan 22, 2024

Actively exploited

vCenter Server contains an out-of-bounds write vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger an out-of-bounds write potentially leading to remote code execution.

EVRS 87 / 100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.994 99.94th percentile · FIRST	CISA DEADLINE Feb 12, 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	0.994 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
vcenter server	≥ 4.0 ≤ 5.5 7.0 8.0	after 5.5	NVD

Sources

Vendor guidance github.com/advisories/GHSA-87j2-5g9j-7jmv

Additional guidance vmware.com/security/advisories/VMSA-2023-0023.html

NVD nvd.nist.gov/vuln/detail/CVE-2023-34048

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2023-38166

Current data evulnable.com/vulnerability-management/cve/CVE-2023-34048

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