

CVE-2021-21972

VMware vCenter Server Remote Code Execution Vulnerability

Exigent
CISA KEV since Nov 3, 2021
Actively exploited
Ransomware use known
Public exploit module (Metasploit)

The vSphere Client (HTML5) contains a remote code execution vulnerability in a vCenter Server plugin. A malicious actor with network access to port 443 may exploit this issue to execute commands with unrestricted privileges on the underlying operating system that hosts vCenter Server. This affects VMware vCenter Server (7.x before 7.0 U1c, 6.7 before 6.7 U3l and 6.5 before 6.5 U3n) and VMware Cloud Foundation (4.x before 4.2 and 3.x before 3.10.1.2).

EVRS 94 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.96th percentile · FIRST	CISA DEADLINE Nov 17, 2021 KEV since 2021 · 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	0.999 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 updates per vendor instructions.
 Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
cloud foundation	$\geq 3.0 < 3.10.1.2$ $\geq 4.0 < 4.2$	3.10.1.2 · 4.2	NVD
vcenter server	6.5 6.7 7.0	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-c9cr-34rr-8gpr	Additional guidance	vmware.com/security/advisories/VMSA-2021-0002.html
NVD	nvd.nist.gov/vuln/detail/CVE-2021-21972	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-9143	Current data	evulnable.com/vulnerability-management/cve/CVE-2021-21972

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