

CVE-2022-22954

VMware Workspace ONE Access and Identity Manager Server-Side Template Injection Vulnerability

Exigent
CISA KEV since Apr 14, 2022
Actively exploited
Ransomware use known
Public exploit module (Metasploit)

VMware Workspace ONE Access and Identity Manager contain a remote code execution vulnerability due to server-side template injection. A malicious actor with network access can trigger a server-side template injection that may result in remote code execution.

EVRS 94 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.99th percentile · FIRST	CISA DEADLINE May 5, 2022 KEV since 2022 · 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
identity manager	3.3.3 3.3.4 3.3.5 3.3.6	no fixed version listed	NVD
vrealize automation	7.6	no fixed version listed	NVD
workspace one access	20.10.0.0 20.10.0.1 21.08.0.0 21.08.0.1	no fixed version listed	NVD
linux kernel	—	no fixed version listed	NVD
cloud foundation	≥ 4.0 ≤ 4.3.1	after 4.3.1	NVD
vrealize suite lifecycle manager	≥ 8.0 ≤ 8.2	after 8.2	NVD

Sources

Vendor guidance github.com/advisories/GHSA-q7xc-35g4-g566

NVD nvd.nist.gov/vuln/detail/CVE-2022-22954

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2022-28077

Additional guidance vmware.com/security/advisories/VMSA-2022-0011.html

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

Current data evulnable.com/vulnerability-management/cve/CVE-2022-22954



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