

CVE-2021-22054

Omnissa Workspace ONE Server-Side Request Forgery

CISA KEV since Mar 9, 2026

Actively exploited

VMware Workspace ONE UEM console 20.0.8 prior to 20.0.8.37, 20.11.0 prior to 20.11.0.40, 21.2.0 prior to 21.2.0.27, and 21.5.0 prior to 21.5.0.37 contain an SSRF vulnerability. This issue may allow a malicious actor with network access to UEM to send their requests without authentication and to gain access to sensitive information.

EVRS 87/100 Immediate priority	CVSS V3.1 7.5 High · NVD	EPSS 0.997 99.95th percentile · FIRST	CISA DEADLINE Mar 23, 2026 CISA federal deadline · Overdue by 7 months
--	--	---	--

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	Added to CISA KEV within the last year
☒ EPSS	0.997 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, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
workspace one uem console	$\geq 20.0.8.0 < 20.0.8.36$ $\geq 20.11.0.0 < 20.11.0.40$ $\geq 21.2.0.0 < 21.2.0.27$ $\geq 21.5.0.0 < 21.5.0.37$	$20.0.8.36 \cdot 20.11.0.40 \cdot 21.2.0.27 \cdot 21.5.0.37$	NVD

Sources

Vendor guidance	vmware.com/security/advisories/VMSA-2021-0029.html	web.archive.org	web.archive.org/web/20211222154335/https://www.vmware.com/security/advisories/VMSA-2021-0029.html
NVD	nvd.nist.gov/vuln/detail/CVE-2021-22054	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-9219	Current data	evulnable.com/vulnerability-management/cve/CVE-2021-22054

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