CVE-2021-22054

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2021-22054
State	PUBLIC
Assigner	security@vmware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-17 17:15:00 UTC
Updated	2021-12-22 03:16:00 UTC
Description	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

Risk And Classification

EPSS: 0.938400000 probability, percentile 0.998690000 (date 2026-05-13)

CISA KEV: Listed on 2026-03-09; due 2026-03-23; ransomware use Unknown

Problem Types: CWE-918

CISA Known Exploited Vulnerability

Vendor	Omnissa
Product	Workspace One UEM
Name	Omnissa Workspace ONE Server-Side Request Forgery
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.
Notes	https://web.archive.org/web/20211222154335/https://www.vmware.com/security/advisories/VMSA-2021-0029.html ; https://nvd.nist.gov/vuln/detail/CVE-2021-22054

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vmware	Workspace One Uem Console	All	All	All	All

References

Reference	Source	Link	Tags
VMSA-2021-0029	MISC	www.vmware.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.