



CVE-2022-22960

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2022-22960
State	PUBLIC
Assigner	security@vmware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-13 18:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a privilege escalation vulnerability du

Risk And Classification

EPSS: 0.704210000 probability, percentile 0.986760000 (date 2026-04-01)

CISA KEV: Listed on 2022-04-15; due 2022-05-06; ransomware use Unknown

Problem Types: CWE-732

CISA Known Exploited Vulnerability

Vendor	VMware
Product	Multiple Products
Name	VMware Multiple Products Privilege Escalation Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2022-22960

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	-	All	All	All
Application	Vmware	Cloud Foundation	All	All	All	All
Application	Vmware	Identity Manager	3.3.3	All	All	All
Application	Vmware	Identity Manager	3.3.4	All	All	All
Application	Vmware	Identity Manager	3.3.5	All	All	All
Application	Vmware	Identity Manager	3.3.6	All	All	All
Application	Vmware	Vrealize Automation	All	All	All	All
Application	Vmware	Vrealize Automation	7.6	All	All	All

Application	Vmware	Vrealize Suite Lifecycle Manager	All	All	All	All
Application	Vmware	Workspace One Access	20.10.0.0	All	All	All
Application	Vmware	Workspace One Access	20.10.0.1	All	All	All
Application	Vmware	Workspace One Access	21.08.0.0	All	All	All
Application	Vmware	Workspace One Access	21.08.0.1	All	All	All

References

Reference	Source	Link	Tags
VMware Workspace ONE Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
VMware Workspace ONE Access Privilege Escalation ≈ Packet Storm	MISC	packetstormsecurity.com	
VMSA-2022-0011	MISC	www.vmware.com	
Mware Workspace ONE Remote Code Execution ≈ Packet Storm	MISC	packetstormsecurity.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.

Legacy QID Mappings

[376521](#) VMware Identity Manager (vIDM) and Workspace ONE Access Multiple Vulnerabilities (VMSA-2022-0011)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report