



CVE-2020-3952

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-3952
State	PUBLIC
Assigner	security@vmware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-10 14:15:00 UTC
Updated	2022-07-12 17:42:00 UTC
Description	Under certain conditions, vmdir that ships with VMware vCenter Server, as part of an embedded or external Platform Service

Risk And Classification

EPSS: 0.943370000 probability, percentile 0.999560000 (date 2026-05-14)

CISA KEV: Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

Problem Types: CWE-306

CISA Known Exploited Vulnerability

Vendor	VMware
Product	vCenter Server
Name	VMware vCenter Server Information Disclosure Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2020-3952

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vmware	Vcenter Server	6.7	-	All	All
Application	Vmware	Vcenter Server	6.7	-	All	All

References

Reference	Source	Link	Tags
VMware vCenter Server 6.7 Authentication Bypass ≈ Packet Storm	MISC	packetstormsecurity.com	
VMSA-2020-0006.1	MISC	www.vmware.com	Vendor Advisory
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.			

© [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](#).

Free CVE JSON API cve.report/api

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