



CVE-2021-21999

Published on: 06/23/2021 12:00:00 AM UTC

Last Modified on: 07/12/2022 05:42:00 PM UTC

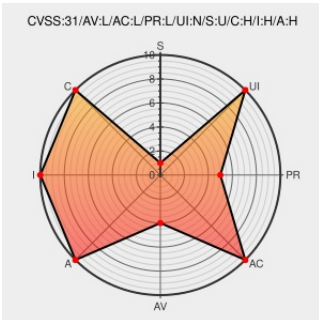
CVE-2021-21999

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [App Volumes](#) from [Vmware](#) contain the following vulnerability:

VMware Tools for Windows (11.x.y prior to 11.2.6), VMware Remote Console for Windows (12.x prior to 12.0.1) , VMware App Volumes (2.x prior to 2.18.10 and 4 prior to 2103) contain a local privilege escalation vulnerability. An attacker with normal access to a virtual machine may exploit this issue by placing a malicious file renamed as `openssl.cnf` in an unrestricted directory which would allow code to be executed with elevated privileges.

CVE-2021-21999 has been assigned by [vmw](#) security@vmware.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.2 - HIGH**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
ZDI-21-754 Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-21-754/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[375665](#) VMware Tools Local Privilege Escalation Vulnerability (VMSA-2021-0013)

[375922](#) VMware Remote Console Local Privilege Escalation Vulnerability (VMSA-2021-0013)








[375939](#) VMware App Volumes Local Privilege Escalation Vulnerability (VMSA-2021-0013)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vmware	App Volumes	All	All	All	All
Application	Vmware	Remote Console	All	All	All	All
Application	Vmware	Tools	All	All	All	All
cpe:2.3:a:vmware:app_volumes:*:*:*:*:*:						
cpe:2.3:a:vmware:remote_console:*:*:*:*:windows:*:*:						
cpe:2.3:a:vmware:tools:*:*:*:*:windows:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @NormanOre	VMSA-2021-0013 CVSSv3 Range:7.8 Issue Date:2021-06-22 CVE(s): CVE-2021-21999 Synopsis: VMware Tools, VMRC and VM... twitter.com/i/web/status/1...	2021-06-22 22:17:27
 @CVEreport	CVE-2021-21999 : VMware Tools for #Windows 11.x.y prior to 11.2.6 , VMware Remote Console for Windows 12.x prior... twitter.com/i/web/status/1...	2021-06-23 12:06:12
 @TristanDostaler	VMware Tools for Windows, VMware Remote Console (VMRC) for Windows and VMware App Volumes CVE-2021-21999 CVSS 7.8 p... twitter.com/i/web/status/1...	2021-06-23 12:50:50
 @threatmeter	CVE-2021-21999 VMware Tools for Windows (11.x.y prior to 11.2.6), VMware Remote Console for Windows (12.x prior to... twitter.com/i/web/status/1...	2021-06-24 07:10:43
 @tempest_sec	As vulnerabilidades foram catalogadas como CVE-2021-21999 (CVSS 7.8) em todos os softwares e, segundo o fabricante,... twitter.com/i/web/status/1...	2021-06-24 12:56:06
 @cKure7	██████ CVE-2021-21999: VMware Workstation Tools Uncontrolled Search Path Element Local Privilege Escalation Vulnerab... twitter.com/i/web/status/1...	2021-06-25 12:25:24
 /r/netcve	CVE-2021-21999	2021-06-23 12:41:26

© [CVE.report](#) 2023   |

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](#)