

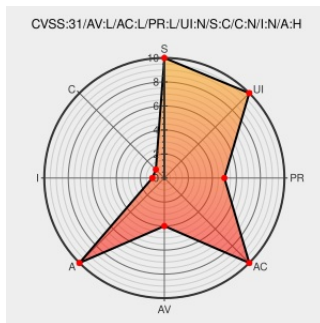


CVE-2020-3999

Published on: 12/21/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-3999

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Mac Os X](#) from [Apple](#) contain the following vulnerability:

VMware ESXi (7.0 prior to ESXi70U1c-17325551), VMware Workstation (16.x prior to 16.0 and 15.x prior to 15.5.7), VMware Fusion (12.x prior to 12.0 and 11.x prior to 11.5.7) and VMware Cloud Foundation contain a denial of service vulnerability due to improper input validation in GuestInfo. A malicious actor with normal user

privilege access to a virtual machine can crash the virtual machine's vmx process leading to a denial of service condition.

CVE-2020-3999 has been assigned by [vmw](#) security@vmware.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **2.1 - LOW**

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

CVE References

Description	Tags	Link
VMware ESXi 7.0 prior to ESXi70U1c-17325551, VMware Workstation 16.x prior to 16.0 and 15.x prior to 15.5.7, VMware Fusion 12.x prior to 12.0 and 11.x prior to 11.5.7, and VMware Cloud Foundation 12.x prior to 12.0 and 11.x prior to 11.5.7 contain a denial of service vulnerability due to improper input validation in GuestInfo. A malicious actor with normal user privilege access to a virtual machine can crash the virtual machine's vmx process leading to a denial of service condition.	CVE-2020-3999	MISC:vmware.com/security/advisories/MISA-2020-0000.html

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

216269 VMware ESXi 7.0 Patch Release ESXi70U1c-17325551 Missing (VMSA-2020-0029)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	-	All	All	All
Operating System	Apple	Mac Os X	-	All	All	All
Operating System	Vmware	Esxi	All	All	All	All
Operating System	Vmware	Esxi	All	All	All	All
Application	Vmware	Fusion	All	All	All	All
Application	Vmware	Fusion	All	All	All	All
Application	Vmware	Workstation	All	All	All	All
Application	Vmware	Workstation	All	All	All	All

cpe:2.3:o:apple:mac_os_x:-:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:-:*:*:*:*:*:

cpe:2.3:o:vmware:esxi:*:*:*:*:*:

cpe:2.3:o:vmware:esxi:*:*:*:*:*:

cpe:2.3:a:vmware:fusion:*:*:*:*:*:

cpe:2.3:a:vmware:fusion:*:*:*:*:*:

cpe:2.3:a:vmware:workstation:*:*:*:*:*:

cpe:2.3:a:vmware:workstation:*:*:*:*:*:

No vendor comments have been submitted for this CVE

© [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](#)