



CVE-2017-4950

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

Summary

CVE	CVE-2017-4950
State	PUBLIC
Assigner	security@vmware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-11 14:29:00 UTC
Updated	2018-02-13 00:35:00 UTC
Description	VMware Workstation and Fusion contain an integer overflow vulnerability in VMware NAT service when IPv6 mode is enabled

Risk And Classification

Problem Types: CWE-190

NVD Known Affected Configurations (CPE 2.3)

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
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

References

Reference
VMSA-2018-0005
Multiple VMware Products CVE-2017-4950 Integer Overflow Vulnerability
VMware Workstation and Fusion Use-After-Free and Integer Overflow Lets Local Users on a Guest System Gain Elevated Privileges on the Host
CVE Program record
NVD vulnerability detail

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](#)