



CVE-2017-4911

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

Summary

CVE	CVE-2017-4911
State	PUBLIC
Assigner	security@vmware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-08 13:29:00 UTC
Updated	2017-07-11 01:33:00 UTC
Description	VMware Workstation (12.x prior to 12.5.3) and Horizon View Client (4.x prior to 4.4.0) contain multiple out-of-bounds write v

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vmware	Horizon View	4.0	All	All	All
Application	Vmware	Horizon View	4.1	All	All	All
Application	Vmware	Horizon View	4.2	All	All	All
Application	Vmware	Horizon View	4.3	All	All	All
Application	Vmware	Horizon View	4.0	All	All	All
Application	Vmware	Horizon View	4.1	All	All	All
Application	Vmware	Horizon View	4.2	All	All	All
Application	Vmware	Horizon View	4.3	All	All	All
Application	Vmware	Workstation	12.0	All	All	All
Application	Vmware	Workstation	12.0.1	All	All	All
Application	Vmware	Workstation	12.1	All	All	All
Application	Vmware	Workstation	12.1.1	All	All	All
Application	Vmware	Workstation	12.5	All	All	All
Application	Vmware	Workstation	12.5.1	All	All	All
Application	Vmware	Workstation	12.5.2	All	All	All
Application	Vmware	Workstation	12.0	All	All	All
Application	Vmware	Workstation	12.0.1	All	All	All

Application	Vmware	Workstation	12.1	All	All	All
Application	Vmware	Workstation	12.1.1	All	All	All
Application	Vmware	Workstation	12.5	All	All	All
Application	Vmware	Workstation	12.5.1	All	All	All
Application	Vmware	Workstation	12.5.2	All	All	All

References

Reference

VMware Workstation and Horizon View Client CVE-2017-4911 Remote Code Execution Vulnerability

VMware Horizon View Buffer Overflows Let Remote Users Execute Arbitrary Code and Guest Users Deny Service and Gain Elevated Privileges

VMware Workstation Heap Overflows Let Local Users on the Guest System Deny Service or Gain Elevated Privileges on the Host System - S

VMSA-2017-0008.2

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](#)