



CVE-2017-4946

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

Summary

CVE	CVE-2017-4946
State	PUBLIC
Assigner	security@vmware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-05 14:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	The VMware V4H and V4PA desktop agents (6.x before 6.5.1) contain a privilege escalation vulnerability. Successful explo

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vmware	Vrealize Operations For Horizon	All	All	All	All
Application	Vmware	Vrealize Operations For Horizon	All	All	All	All
Application	Vmware	Vrealize Operations For Published Applications	All	All	All	All
Application	Vmware	Vrealize Operations For Published Applications	All	All	All	All

References

Reference
Multiple VMware Products Multiple Security Vulnerabilities
VMware Horizon (V4H/V4PA) desktop agent privilege escalation vulnerability (CVE-2017-4946) :: GoSecure
VMware vRealize Operations for Horizon and vRealize Operations for Published Applications Lets Local Users Obtain System Privileges - Sec
VMSA-2018-0003
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](#)