



CVE-2017-4919

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

Summary

CVE	CVE-2017-4919
State	PUBLIC
Assigner	security@vmware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-28 22:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	VMware vCenter Server 5.5, 6.0, 6.5 allows vSphere users with certain, limited vSphere privileges to use the VIX API to ac

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vmware	Vcenter Server	5.5	All	All	All
Application	Vmware	Vcenter Server	6.0	All	All	All
Application	Vmware	Vcenter Server	6.5	All	All	All
Application	Vmware	Vcenter Server	5.5	All	All	All
Application	Vmware	Vcenter Server	6.0	All	All	All
Application	Vmware	Vcenter Server	6.5	All	All	All

References

Reference

VMware vCenter Server CVE-2017-4919 Local Authentication Bypass Vulnerability
VMware vCenter Server VIX API Direct Access Function Lets Remote Authenticated vSphere Users Access the Target Guest System - Secur
VMSA-2017-0012
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](#)