



CVE-2017-4927

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

Summary

CVE	CVE-2017-4927
State	PUBLIC
Assigner	security@vmware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-17 14:29:00 UTC
Updated	2017-12-04 16:30:00 UTC
Description	VMware vCenter Server (6.5 prior to 6.5 U1 and 6.0 prior to 6.0 U3c) does not correctly handle specially crafted LDAP network requests, which may allow remote attackers to cause a denial of service (service crash) via a crafted LDAP request.

Risk And Classification

Problem Types: CWE-90

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source
VMware vCenter Server CVE-2017-4927 Denial of Service Vulnerability	BID
VMware vCenter Server Flaws Let Remote Users Deny Service and Obtain Potentially Sensitive Information - SecurityTracker	SECTrack
VMSA-2017-0017	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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