



CVE-2014-3796

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

Summary

CVE	CVE-2014-3796
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-09-15 14:55:11 UTC
Updated	2026-05-06 22:30:45 UTC
Description	VMware NSX 6.0 before 6.0.6, and vCloud Networking and Security (vCNS) 5.1 before 5.1.4.2 and 5.5 before 5.5.3, does not properly validate the format of the NSX Manager API request, which allows remote attackers to execute arbitrary code or cause a denial of service (memory consumption) via a crafted request.

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:N/A:N

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:L/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	VMware	NSX	6.0	All	All	All

Application	Vmware	Nsx	6.0.1	All	All	All
Application	Vmware	Nsx	6.0.2	All	All	All
Application	Vmware	Nsx	6.0.3	All	All	All
Application	Vmware	Nsx	6.0.4	All	All	All
Application	Vmware	Nsx	6.0.5	All	All	All
Application	Vmware	Vcloud Networking And Security	5.1	All	All	All
Application	Vmware	Vcloud Networking And Security	5.1.1	All	All	All
Application	Vmware	Vcloud Networking And Security	5.1.2	All	All	All
Application	Vmware	Vcloud Networking And Security	5.1.3	All	All	All
Application	Vmware	Vcloud Networking And Security	5.1.4	All	All	All
Application	Vmware	Vcloud Networking And Security	5.1.4.1	All	All	All
Application	Vmware	Vcloud Networking And Security	5.5	All	All	All
Application	Vmware	Vcloud Networking And Security	5.5.0a	All	All	All
Application	Vmware	Vcloud Networking And Security	5.5.1	All	All	All
Application	Vmware	Vcloud Networking And Security	5.5.2	All	All	All
Application	Vmware	Vcloud Networking And Security	5.5.2.1	All	All	All

Vendor Declared Affected Products					
Source	Vendor	Product	Version	Platforms	
CNA	Na	N/a	affected n/a	Not specified	

References	
Reference	Source
IBM X-Force Exchange	a
Security Advisory SA59938 - VMware NSX / vCloud Networking and Security (vCNS) Information Disclosure Vulnerability - Secunia	a
VMSA-2014-0009 United States	a
VMware vCloud Networking and Security (vCNS) Input Validation Flaw Lets Remote Users Obtain Sensitive Information - SecurityTracker	a
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

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

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