



CVE-2014-3367

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

Summary

CVE	CVE-2014-3367
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-09-20 10:55:00 UTC
Updated	2017-08-29 01:34:00 UTC
Description	Cross-site scripting (XSS) vulnerability in the vCloud Director component in Cisco Nexus 1000V InterCloud for VMware allo

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Cisco Nexus 1000v Intercloud	-	All	All	All
Application	Cisco	Cisco Nexus 1000v Intercloud	-	All	All	All

References

Reference	Source	Link
IBM X-Force Exchange	XF	exchange.xforce.it
Cisco Nexus 1000V CVE-2014-3367 Cross Site Scripting Vulnerability	BID	www.securityfocus
Cisco NX-OS Nexus 1000V Input Validation Hole Permits Cross-Site Scripting Attacks - SecurityTracker	SECTrack	www.securitytrack
20140919 Cisco Nexus 1000V Cross-Site Scripting Vulnerability	CISCO	tools.cisco.com
Security Advisory SA61426 - Cisco Nexus 1000V Unspecified Cross-Site Scripting Vulnerability - Secunia	SECUNIA	secunia.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)