

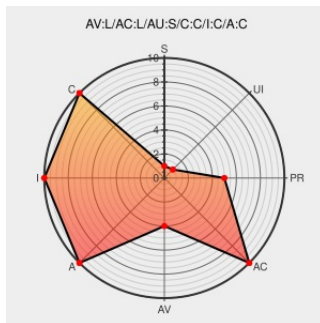


CVE-2013-5556

Published on: 11/15/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:35 PM UTC

CVE-2013-5556

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Nexus 1000v](#) from [Cisco](#) contain the following vulnerability:

The license-installation module on the Cisco Nexus 1000V switch 4.2(1)SV1(5.2b) and earlier for VMware vSphere, Cisco Nexus 1000V switch 5.2(1)SM1(5.1) for Microsoft Hyper-V, and Cisco Virtual Security Gateway 4.2(1)VSG1(1) for Nexus 1000V switches allows local users to gain privileges and execute arbitrary commands via crafted "install all iso" arguments, aka Bug ID CSCui21340.

CVE-2013-5556 has been assigned by [psirt@cisco.com](#) to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Alert Details - Security Center - Cisco Systems	Vendor Advisory tools.cisco.com text/html	CONFIRM tools.cisco.com/security/center/viewAlert.x?alertId=31774
Cisco Security Notice: Cisco Nexus 1000V Arbitrary Command Execution Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20131114 Cisco Nexus 1000V Arbitrary Command Execution Vulnerability

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](#).

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware  	Cisco	Nexus 1000v	4.2(1)sv1(5.1)	-	All	All
Hardware  	Cisco	Nexus 1000v	4.2(1)sv1(5.1a)	-	All	All
Hardware  	Cisco	Nexus 1000v	4.2(1)sv1(5.2)	-	All	All
Hardware  	Cisco	Nexus 1000v	4.2(1)vsg1(1)	-	All	All
Hardware  	Cisco	Nexus 1000v	4.2(1)_sv1(4)	-	All	All
Hardware  	Cisco	Nexus 1000v	4.2(1)_sv1(4a)	-	All	All
Hardware  	Cisco	Nexus 1000v	4.2(1)_sv1(4b)	-	All	All
Hardware  	Cisco	Nexus 1000v	4.2(1)sv1(5.1a)	-	All	All
Hardware  	Cisco	Nexus 1000v	4.2(1)sv1(5.1)	-	All	All
Hardware  	Cisco	Nexus 1000v	4.2(1)sv1(5.2)	-	All	All
Hardware  	Cisco	Nexus 1000v	4.2(1)vsg1(1)	-	All	All
Hardware  	Cisco	Nexus 1000v	4.2(1)_sv1(4a)	-	All	All
Hardware  	Cisco	Nexus 1000v	4.2(1)_sv1(4b)	-	All	All
Hardware  	Cisco	Nexus 1000v	4.2(1)_sv1(4)	-	All	All
Hardware  	Cisco	Nexus 1000v	5.2(1)sm1(5.1)	-	All	All
Hardware  	Cisco	Nexus 1000v	5.2(1)sm1(5.1)	-	All	All
Hardware  	Cisco	Nexus 1000v	4.2(1)sv1(5.1a)	-	All	All
Hardware  	Cisco	Nexus 1000v	4.2(1)sv1(5.1)	-	All	All
Hardware  	Cisco	Nexus 1000v	4.2(1)sv1(5.2)	-	All	All
Hardware  	Cisco	Nexus 1000v	4.2(1)vsg1(1)	-	All	All
Hardware  	Cisco	Nexus 1000v	4.2(1)_sv1(4a)	-	All	All
Hardware  	Cisco	Nexus 1000v	4.2(1)_sv1(4b)	-	All	All
Hardware  	Cisco	Nexus 1000v	4.2(1)_sv1(4)	-	All	All
Hardware  	Cisco	Nexus 1000v	5.2(1)sm1(5.1)	-	All	All
Hardware  	Cisco	Nexus 1000v	All	-	All	All
Hardware  	Cisco	Nexus 1000v	All	-	All	All

cpe:2.3:h:cisco:nexus_1000v:4.2(1)sv1(5.1):-:*:*:vmware_vsphere:*:*:

cpe:2.3:h:cisco:nexus_1000v:4.2(1)sv1(5.1a):-:*:*:vmware_vsphere:*:*:
cpe:2.3:h:cisco:nexus_1000v:4.2(1)sv1(5.2):-:*:*:vmware_vsphere:*:*:
cpe:2.3:h:cisco:nexus_1000v:4.2(1)vsg1(1):-:*:*:nexus_1000v:*:*:
cpe:2.3:h:cisco:nexus_1000v:4.2(1)_sv1(4):-:*:*:vmware_vsphere:*:*:
cpe:2.3:h:cisco:nexus_1000v:4.2(1)_sv1(4a):-:*:*:vmware_vsphere:*:*:
cpe:2.3:h:cisco:nexus_1000v:4.2(1)_sv1(4b):-:*:*:vmware_vsphere:*:*:
cpe:2.3:h:cisco:nexus_1000v:4.2(1)sv1(5.1a):-:*:*:vmware_vsphere:*:*:
cpe:2.3:h:cisco:nexus_1000v:4.2(1)sv1(5.1):-:*:*:vmware_vsphere:*:*:
cpe:2.3:h:cisco:nexus_1000v:4.2(1)sv1(5.2):-:*:*:vmware_vsphere:*:*:
cpe:2.3:h:cisco:nexus_1000v:4.2(1)vsg1(1):-:*:*:nexus_1000v:*:*:
cpe:2.3:h:cisco:nexus_1000v:4.2(1)_sv1(4a):-:*:*:vmware_vsphere:*:*:
cpe:2.3:h:cisco:nexus_1000v:4.2(1)_sv1(4b):-:*:*:vmware_vsphere:*:*:
cpe:2.3:h:cisco:nexus_1000v:4.2(1)_sv1(4):-:*:*:vmware_vsphere:*:*:
cpe:2.3:h:cisco:nexus_1000v:5.2(1)sm1(5.1):-:*:*:microsoft_hyper-v:*:*:
cpe:2.3:h:cisco:nexus_1000v:5.2(1)sm1(5.1):-:*:*:microsoft_hyper-v:*:*:
cpe:2.3:h:cisco:nexus_1000v:4.2(1)sv1(5.1a):-:*:*:vmware_vsphere:*:*:
cpe:2.3:h:cisco:nexus_1000v:4.2(1)sv1(5.1):-:*:*:vmware_vsphere:*:*:
cpe:2.3:h:cisco:nexus_1000v:4.2(1)sv1(5.2):-:*:*:vmware_vsphere:*:*:
cpe:2.3:h:cisco:nexus_1000v:4.2(1)vsg1(1):-:*:*:nexus_1000v:*:*:
cpe:2.3:h:cisco:nexus_1000v:4.2(1)_sv1(4a):-:*:*:vmware_vsphere:*:*:
cpe:2.3:h:cisco:nexus_1000v:4.2(1)_sv1(4b):-:*:*:vmware_vsphere:*:*:
cpe:2.3:h:cisco:nexus_1000v:4.2(1)_sv1(4):-:*:*:vmware_vsphere:*:*:
cpe:2.3:h:cisco:nexus_1000v:5.2(1)sm1(5.1):-:*:*:microsoft_hyper-v:*:*:
cpe:2.3:h:cisco:nexus_1000v:*:*:*:vmware_vsphere:*:*:
cpe:2.3:h:cisco:nexus_1000v:*:*:*:vmware_vsphere:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)