



CVE-2017-12341

Published on: 11/30/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:30 PM UTC

CVE-2017-12341

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

CVSS:30/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Nx-os](#) from [Cisco](#) contain the following vulnerability:

A vulnerability in the CLI of Cisco NX-OS System Software could allow an authenticated, local attacker to perform a command injection attack. An attacker would need valid administrator credentials to perform this exploit. The vulnerability is due to insufficient input validation during the installation of a software patch. An attacker could exploit this vulnerability by installing a crafted patch image with the vulnerable

operation occurring prior to patch activation. An exploit could allow the attacker to execute arbitrary commands on an affected system as root. This vulnerability affects the following products running Cisco NX-OS System Software: Multilayer Director Switches, Nexus 2000 Series Fabric Extenders, Nexus 5000 Series Switches, Nexus 5500 Platform Switches, Nexus 5600 Platform Switches, Nexus 6000 Series Switches, Nexus 7000 Series Switches, Nexus 7700 Series Switches, Unified Computing System Manager. Cisco Bug IDs: CSCvf23735, CSCvg04072.

CVE-2017-12341 has been assigned by [cisco](#) psirt@cisco.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.7 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	HIGH	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.2 - HIGH**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

COMPLETE

COMPLETE

COMPLETE

CVE References

Description	Tags	Link
Cisco NX-OS CLI Patch Installation Bug Lets Local Users Gain Root Privileges - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	 SECTrack 1039939
Cisco NX-OS System Software Patch Installation Command Injection Vulnerability	Vendor Advisory tools.cisco.com text/html	 CONFIRM tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171129-nxos8

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
Operating System	Cisco	Nx-os	8.1(0.59)s0	All	All	All
Operating System	Cisco	Nx-os	8.1(1)	All	All	All
Operating System	Cisco	Nx-os	8.1(0.59)s0	All	All	All
Operating System	Cisco	Nx-os	8.1(1)	All	All	All
Operating System	Cisco	Nx-os	8.1(0.59)s0	All	All	All
Operating System	Cisco	Nx-os	8.1(1)	All	All	All
Application	Cisco	Unified Computing System	7.0(0)hsk(0.357)	All	All	All
Application	Cisco	Unified Computing System	7.0(0)hsk(0.357)	All	All	All
Application	Cisco	Unified Computing System	7.0(0)hsk(0.357)	All	All	All

```
cpe:2.3:o:cisco:nx-os:8.1(0.59)s0:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:nx-os:8.1(1):*:*:*:*:*:
```

```
cpe:2.3:o:cisco:nx-os:8.1(0.59)\s0:*.:.:.:.:.:
```

```
cpe:2.3:o:cisco:nx-os:8.1\(\1\):*:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:nx-os:8.1(0.59)\s0:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:cisco:nx-os:8.1(1\):*:*:*:*:*:*:
```

cpe:2.3:a:cisco:unified_computing_system:7.0(0)hsk(0.357):*:~::~:	
cpe:2.3:a:cisco:unified_computing_system:7.0(0)hsk(0.357):*:~::~:	
cpe:2.3:a:cisco:unified_computing_system:7.0(0)hsk(0.357):*:~::~:	
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