



# CVE-2017-12301

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-12301
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-10-19 08:29:00 UTC
<b>Updated</b>	2019-10-09 23:22:00 UTC
<b>Description</b>	A vulnerability in the Python scripting subsystem of Cisco NX-OS Software could allow an authenticated, local attacker to e

## Risk And Classification

### Problem Types: CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Multilayer Director	-	All	All	All
Hardware	Cisco	Multilayer Director	-	All	All	All
Hardware	Cisco	Nexus 2000	-	All	All	All
Hardware	Cisco	Nexus 2000	-	All	All	All
Hardware	Cisco	Nexus 3000	-	All	All	All
Hardware	Cisco	Nexus 3000	-	All	All	All
Hardware	Cisco	Nexus 3016	-	All	All	All
Hardware	Cisco	Nexus 3016	-	All	All	All
Hardware	Cisco	Nexus 3016q	-	All	All	All
Hardware	Cisco	Nexus 3016q	-	All	All	All
Hardware	Cisco	Nexus 3048	-	All	All	All
Hardware	Cisco	Nexus 3048	-	All	All	All
Hardware	Cisco	Nexus 3064	-	All	All	All
Hardware	Cisco	Nexus 3064	-	All	All	All
Hardware	Cisco	Nexus 3064t	-	All	All	All
Hardware	Cisco	Nexus 3064t	-	All	All	All
Hardware	Cisco	Nexus 3064x	-	All	All	All

Hardware	Cisco	Nexus 3064x	-	All	All	All
Hardware	Cisco	Nexus 3500	-	All	All	All
Hardware	Cisco	Nexus 3500	-	All	All	All
Hardware	Cisco	Nexus 3524	-	All	All	All
Hardware	Cisco	Nexus 3524	-	All	All	All
Hardware	Cisco	Nexus 3548	-	All	All	All
Hardware	Cisco	Nexus 3548	-	All	All	All
Hardware	Cisco	Nexus 5000	-	All	All	All
Hardware	Cisco	Nexus 5000	-	All	All	All
Hardware	Cisco	Nexus 5010	-	All	All	All
Hardware	Cisco	Nexus 5010	-	All	All	All
Hardware	Cisco	Nexus 5010p Switch	-	All	All	All
Hardware	Cisco	Nexus 5010p Switch	-	All	All	All
Hardware	Cisco	Nexus 5500	-	All	All	All
Hardware	Cisco	Nexus 5500	-	All	All	All
Hardware	Cisco	Nexus 5548p	-	All	All	All
Hardware	Cisco	Nexus 5548p	-	All	All	All
Hardware	Cisco	Nexus 5548up	-	All	All	All
Hardware	Cisco	Nexus 5548up	-	All	All	All
Hardware	Cisco	Nexus 5596t	-	All	All	All
Hardware	Cisco	Nexus 5596t	-	All	All	All
Hardware	Cisco	Nexus 5596up	-	All	All	All
Hardware	Cisco	Nexus 5596up	-	All	All	All
Hardware	Cisco	Nexus 5600	-	All	All	All
Hardware	Cisco	Nexus 5600	-	All	All	All
Hardware	Cisco	Nexus 56128p	-	All	All	All
Hardware	Cisco	Nexus 56128p	-	All	All	All
Hardware	Cisco	Nexus 5624q	-	All	All	All
Hardware	Cisco	Nexus 5624q	-	All	All	All
Hardware	Cisco	Nexus 5648q	-	All	All	All
Hardware	Cisco	Nexus 5648q	-	All	All	All
Hardware	Cisco	Nexus 5672up	-	All	All	All
Hardware	Cisco	Nexus 5672up	-	All	All	All
Hardware	Cisco	Nexus 5696q	-	All	All	All
Hardware	Cisco	Nexus 5696q	-	All	All	All

Hardware	Cisco	Nexus 6000	-	All	All	All
Hardware	Cisco	Nexus 6000	-	All	All	All
Hardware	Cisco	Nexus 6001	-	All	All	All
Hardware	Cisco	Nexus 6001	-	All	All	All
Hardware	Cisco	Nexus 6004	-	All	All	All
Hardware	Cisco	Nexus 6004	-	All	All	All
Hardware	Cisco	Nexus 6004x	-	All	All	All
Hardware	Cisco	Nexus 6004x	-	All	All	All
Hardware	Cisco	Nexus 7000	-	All	All	All
Hardware	Cisco	Nexus 7000	-	All	All	All
Hardware	Cisco	Nexus 7000 10-slot	-	All	All	All
Hardware	Cisco	Nexus 7000 10-slot	-	All	All	All
Hardware	Cisco	Nexus 7000 18-slot	-	All	All	All
Hardware	Cisco	Nexus 7000 18-slot	-	All	All	All
Hardware	Cisco	Nexus 7000 9-slot	-	All	All	All
Hardware	Cisco	Nexus 7000 9-slot	-	All	All	All
Hardware	Cisco	Nexus 7700	-	All	All	All
Hardware	Cisco	Nexus 7700	-	All	All	All
Hardware	Cisco	Nexus 9000	-	All	All	All
Hardware	Cisco	Nexus 9000	-	All	All	All
Hardware	Cisco	Nexus 9500 R	-	All	All	All
Hardware	Cisco	Nexus 9500 R	-	All	All	All
Operating System	Cisco	Nx-os	6.0(2)a8(3)	All	All	All
Operating System	Cisco	Nx-os	6.0(2)a8(6.213)	All	All	All
Operating System	Cisco	Nx-os	6.0(2)a8(3)	All	All	All
Operating System	Cisco	Nx-os	6.0(2)a8(6.213)	All	All	All
Operating System	Cisco	Nx-os	7.0(0)hsk(0.357)	All	All	All
Operating System	Cisco	Nx-os	7.0(3)i4(6)	All	All	All
Operating System	Cisco	Nx-os	7.0(0)hsk(0.357)	All	All	All
Operating System	Cisco	Nx-os	7.0(3)i4(6)	All	All	All
Operating System	Cisco	Nx-os	7.3(2)d1(0.21)	All	All	All
Operating System	Cisco	Nx-os	7.3(2)d1(0.21)	All	All	All
Operating System	Cisco	Nx-os	8.0(0.74)	All	All	All
Operating System	Cisco	Nx-os	8.0(1)	All	All	All
Operating System	Cisco	Nx-os	8.0(0.74)	All	All	All

Operating System	Cisco	Nx-os	8.0(1)	All	All	All
Operating System	Cisco	Nx-os	8.1(0)bd(0.20)	All	All	All
Operating System	Cisco	Nx-os	8.1(0.70)s0	All	All	All
Operating System	Cisco	Nx-os	8.1(0.70)s0	All	All	All
Operating System	Cisco	Nx-os	8.1(0)bd(0.20)	All	All	All
Operating System	Cisco	Nx-os	6.0(2)a8(3)	All	All	All
Operating System	Cisco	Nx-os	6.0(2)a8(6.213)	All	All	All
Operating System	Cisco	Nx-os	7.0(0)hsk(0.357)	All	All	All
Operating System	Cisco	Nx-os	7.0(3)i4(6)	All	All	All
Operating System	Cisco	Nx-os	7.3(2)d1(0.21)	All	All	All
Operating System	Cisco	Nx-os	8.0(0.74)	All	All	All
Operating System	Cisco	Nx-os	8.0(1)	All	All	All
Operating System	Cisco	Nx-os	8.1(0.70)s0	All	All	All
Operating System	Cisco	Nx-os	8.1(0)bd(0.20)	All	All	All

## References

Reference	Source
Cisco NX-OS Software Python Parser Escape Vulnerability	CONFIRM
Cisco NX-OS Input Validation Flaw in Python Scripting Sandbox Lets Local Users Gain Elevated Privileges - SecurityTracker	SECTRACK
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.

© 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](#).

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