



# CVE-2019-1727

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

## Summary

<b>CVE</b>	CVE-2019-1727
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-05-15 17:29:00 UTC
<b>Updated</b>	2020-10-16 13:09:00 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-78

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Mds 9000	-	All	All	All
Hardware	Cisco	Mds 9000	-	All	All	All
Hardware	Cisco	Mds 9100	-	All	All	All
Hardware	Cisco	Mds 9100	-	All	All	All
Hardware	Cisco	Mds 9200	-	All	All	All
Hardware	Cisco	Mds 9200	-	All	All	All
Hardware	Cisco	Mds 9500	-	All	All	All
Hardware	Cisco	Mds 9500	-	All	All	All
Hardware	Cisco	Mds 9700	-	All	All	All
Hardware	Cisco	Mds 9700	-	All	All	All
Hardware	Cisco	Nexus 3000	-	All	All	All
Hardware	Cisco	Nexus 3000	-	All	All	All
Hardware	Cisco	Nexus 3100	-	All	All	All
Hardware	Cisco	Nexus 3100	-	All	All	All
Hardware	Cisco	Nexus 3100-z	-	All	All	All
Hardware	Cisco	Nexus 3100-z	-	All	All	All
Hardware	Cisco	Nexus 3100v	-	All	All	All

Hardware	Cisco	Nexus 3100v	-	All	All	All
Hardware	Cisco	Nexus 3200	-	All	All	All
Hardware	Cisco	Nexus 3200	-	All	All	All
Hardware	Cisco	Nexus 3400	-	All	All	All
Hardware	Cisco	Nexus 3400	-	All	All	All
Hardware	Cisco	Nexus 3500	-	All	All	All
Hardware	Cisco	Nexus 3500	-	All	All	All
Hardware	Cisco	Nexus 3524-x	-	All	All	All
Hardware	Cisco	Nexus 3524-x	-	All	All	All
Hardware	Cisco	Nexus 3524-xl	-	All	All	All
Hardware	Cisco	Nexus 3524-xl	-	All	All	All
Hardware	Cisco	Nexus 3548-x	-	All	All	All
Hardware	Cisco	Nexus 3548-x	-	All	All	All
Hardware	Cisco	Nexus 3548-xl	-	All	All	All
Hardware	Cisco	Nexus 3548-xl	-	All	All	All
Hardware	Cisco	Nexus 3600	-	All	All	All
Hardware	Cisco	Nexus 3600	-	All	All	All
Hardware	Cisco	Nexus 5500	-	All	All	All
Hardware	Cisco	Nexus 5500	-	All	All	All
Hardware	Cisco	Nexus 5600	-	All	All	All
Hardware	Cisco	Nexus 5600	-	All	All	All
Hardware	Cisco	Nexus 6000	-	All	All	All
Hardware	Cisco	Nexus 6000	-	All	All	All
Hardware	Cisco	Nexus 7000	-	All	All	All
Hardware	Cisco	Nexus 7000	-	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 9200	-	All	All	All
Hardware	Cisco	Nexus 9200	-	All	All	All
Hardware	Cisco	Nexus 9300	-	All	All	All
Hardware	Cisco	Nexus 9300	-	All	All	All
Hardware	Cisco	Nexus 9500	-	All	All	All
Hardware	Cisco	Nexus 9500	-	All	All	All

Operating System	Cisco	Nx-os	All	All	All	All
Operating System	Cisco	Nx-os	All	All	All	All

## References

Reference	Source	Link	Tags
Cisco NX-OS Software Python Parser Privilege Escalation Vulnerability	CISCO	<a href="https://tools.cisco.com">tools.cisco.com</a>	Vendor Advisory
Cisco NX-OS Software CVE-2019-1727 Local Privilege Escalation Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>	Third Party Advisory
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

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](https://status.cve.report)