



CVE-2019-1615

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

Summary

CVE	CVE-2019-1615
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-11 21:29:00 UTC
Updated	2019-10-09 23:47:00 UTC
Description	A vulnerability in the Image Signature Verification feature of Cisco NX-OS Software could allow an authenticated, local attac

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	9432pq	-	All	All	All
Hardware	Cisco	9432pq	-	All	All	All
Hardware	Cisco	9536pq	-	All	All	All
Hardware	Cisco	9536pq	-	All	All	All
Hardware	Cisco	9636pq	-	All	All	All
Hardware	Cisco	9636pq	-	All	All	All
Hardware	Cisco	9736pq	-	All	All	All
Hardware	Cisco	9736pq	-	All	All	All
Hardware	Cisco	N3k-c31128pq-10ge	-	All	All	All
Hardware	Cisco	N3k-c31128pq-10ge	-	All	All	All
Hardware	Cisco	N3k-c3132c-z	-	All	All	All
Hardware	Cisco	N3k-c3132c-z	-	All	All	All
Hardware	Cisco	N3k-c3164q-40ge	-	All	All	All
Hardware	Cisco	N3k-c3164q-40ge	-	All	All	All
Hardware	Cisco	N3k-c3264q	-	All	All	All
Hardware	Cisco	N3k-c3264q	-	All	All	All
Hardware	Cisco	N9k-x9432c-s	-	All	All	All

Hardware	Cisco	N9k-x9432c-s	-	All	All	All
Hardware	Cisco	N9k-x9464px	-	All	All	All
Hardware	Cisco	N9k-x9464px	-	All	All	All
Hardware	Cisco	N9k-x9464tx2	-	All	All	All
Hardware	Cisco	N9k-x9464tx2	-	All	All	All
Hardware	Cisco	N9k-x9564px	-	All	All	All
Hardware	Cisco	N9k-x9564px	-	All	All	All
Hardware	Cisco	N9k-x9564tx	-	All	All	All
Hardware	Cisco	N9k-x9564tx	-	All	All	All
Hardware	Cisco	N9k-x9636c-r	-	All	All	All
Hardware	Cisco	N9k-x9636c-r	-	All	All	All
Hardware	Cisco	N9k-x9636c-rx	-	All	All	All
Hardware	Cisco	N9k-x9636c-rx	-	All	All	All
Hardware	Cisco	N9k-x97160yc-ex	-	All	All	All
Hardware	Cisco	N9k-x97160yc-ex	-	All	All	All
Hardware	Cisco	N9k-x9732c-ex	-	All	All	All
Hardware	Cisco	N9k-x9732c-ex	-	All	All	All
Hardware	Cisco	N9k-x9732c-fx	-	All	All	All
Hardware	Cisco	N9k-x9732c-fx	-	All	All	All
Hardware	Cisco	N9k-x9736c-ex	-	All	All	All
Hardware	Cisco	N9k-x9736c-ex	-	All	All	All
Hardware	Cisco	N9k-x9736c-fx	-	All	All	All
Hardware	Cisco	N9k-x9736c-fx	-	All	All	All
Hardware	Cisco	N9k-x9788tc-fx	-	All	All	All
Hardware	Cisco	N9k-x9788tc-fx	-	All	All	All
Hardware	Cisco	Nexus 92160yc-x	-	All	All	All
Hardware	Cisco	Nexus 92160yc-x	-	All	All	All
Hardware	Cisco	Nexus 92300yc	-	All	All	All
Hardware	Cisco	Nexus 92300yc	-	All	All	All
Hardware	Cisco	Nexus 92304qc	-	All	All	All
Hardware	Cisco	Nexus 92304qc	-	All	All	All
Hardware	Cisco	Nexus 9236c	-	All	All	All
Hardware	Cisco	Nexus 9236c	-	All	All	All
Hardware	Cisco	Nexus 9272q	-	All	All	All
Hardware	Cisco	Nexus 9272q	-	All	All	All

Hardware	Cisco	Nexus 93108tc-ex	-	All	All	All
Hardware	Cisco	Nexus 93108tc-ex	-	All	All	All
Hardware	Cisco	Nexus 93108tc-fx	-	All	All	All
Hardware	Cisco	Nexus 93108tc-fx	-	All	All	All
Hardware	Cisco	Nexus 93120tx	-	All	All	All
Hardware	Cisco	Nexus 93120tx	-	All	All	All
Hardware	Cisco	Nexus 9316d-gx	-	All	All	All
Hardware	Cisco	Nexus 9316d-gx	-	All	All	All
Hardware	Cisco	Nexus 93180lc-ex	-	All	All	All
Hardware	Cisco	Nexus 93180lc-ex	-	All	All	All
Hardware	Cisco	Nexus 93180yc-ex	-	All	All	All
Hardware	Cisco	Nexus 93180yc-ex	-	All	All	All
Hardware	Cisco	Nexus 93180yc-fx	-	All	All	All
Hardware	Cisco	Nexus 93180yc-fx	-	All	All	All
Hardware	Cisco	Nexus 93240yc-fx2	-	All	All	All
Hardware	Cisco	Nexus 93240yc-fx2	-	All	All	All
Hardware	Cisco	Nexus 9332c	-	All	All	All
Hardware	Cisco	Nexus 9332c	-	All	All	All
Hardware	Cisco	Nexus 9336c-fx2	-	All	All	All
Hardware	Cisco	Nexus 9336c-fx2	-	All	All	All
Hardware	Cisco	Nexus 9348gc-fxp	-	All	All	All
Hardware	Cisco	Nexus 9348gc-fxp	-	All	All	All
Hardware	Cisco	Nexus 93600cd-gx	-	All	All	All
Hardware	Cisco	Nexus 93600cd-gx	-	All	All	All
Hardware	Cisco	Nexus 9364c	-	All	All	All
Hardware	Cisco	Nexus 9364c	-	All	All	All
Hardware	Cisco	Nexus 9504	-	All	All	All
Hardware	Cisco	Nexus 9504	-	All	All	All
Hardware	Cisco	Nexus 9508	-	All	All	All
Hardware	Cisco	Nexus 9508	-	All	All	All
Hardware	Cisco	Nexus 9516	-	All	All	All
Hardware	Cisco	Nexus 9516	-	All	All	All
Operating System	Cisco	Nx-os	12.3(0.97)	All	All	All
Operating System	Cisco	Nx-os	12.3(0.97)	All	All	All
Operating System	Cisco	Nx-os	7.0(3)i7(3)	All	All	All
Operating System	Cisco	Nx-os	7.0(3)i7(3)	All	All	All

Operating System	Cisco	Nx-os	7.0(3)17(5)	All	All	All
Operating System	Cisco	Nx-os	7.0(3)17(3)	All	All	All
Operating System	Cisco	Nx-os	7.0(3)17(5)	All	All	All
Operating System	Cisco	Nx-os	9.2(1)	All	All	All
Operating System	Cisco	Nx-os	9.2(1)	All	All	All
Operating System	Cisco	Nx-os	12.3(0.97)	All	All	All
Operating System	Cisco	Nx-os	7.0(3)17(3)	All	All	All
Operating System	Cisco	Nx-os	7.0(3)17(5)	All	All	All
Operating System	Cisco	Nx-os	9.2(1)	All	All	All
Hardware	Cisco	X9636q-r	-	All	All	All
Hardware	Cisco	X9636q-r	-	All	All	All

References

Reference	Source	Link	Tags
Cisco NX-OS Software CVE-2019-1615 Local Security Bypass Vulnerability	BID	www.securityfocus.com	Third Party Advisory, VC
Cisco NX-OS Software Image Signature Verification Vulnerability	CISCO	tools.cisco.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve/). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report