



CVE-2011-2581

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

Summary

CVE	CVE-2011-2581
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-09-14 16:05:00 UTC
Updated	2022-04-05 15:52:00 UTC
Description	The ACL implementation in Cisco NX-OS 5.0(2) and 5.0(3) before 5.0(3)N2(1) on Nexus 5000 series switches, and NX-OS

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Nexus 3000	All	All	All	All
Hardware	Cisco	Nexus 3000	All	All	All	All
Hardware	Cisco	Nexus 5000	All	All	All	All
Hardware	Cisco	Nexus 5000	All	All	All	All
Application	Cisco	Nx-os	5.0(2)	All	All	All
Application	Cisco	Nx-os	5.0(3)	All	All	All
Application	Cisco	Nx-os	5.0(3)n1(1)	All	All	All
Application	Cisco	Nx-os	5.0(3)n1(1a)	All	All	All
Application	Cisco	Nx-os	5.0(3)n1(1b)	All	All	All
Application	Cisco	Nx-os	5.0(3)n1(1c)	All	All	All
Application	Cisco	Nx-os	5.0(3)u1(1a)	All	All	All
Application	Cisco	Nx-os	5.0(3)u1(1b)	All	All	All
Application	Cisco	Nx-os	5.0(3)u1(1d)	All	All	All
Application	Cisco	Nx-os	5.0\2\	All	All	All
Application	Cisco	Nx-os	5.0\3\	All	All	All
Application	Cisco	Nx-os	5.0\3\ n1\1a\	All	All	All
Application	Cisco	Nx-os	5.0\3\ n1\1b\	All	All	All

Application	Cisco	Nx-os	5.0\3)n1\1c\	All	All	All
Application	Cisco	Nx-os	5.0\3)n1\1\	All	All	All
Application	Cisco	Nx-os	5.0\3)u1\1a\	All	All	All
Application	Cisco	Nx-os	5.0\3)u1\1b\	All	All	All
Application	Cisco	Nx-os	5.0\3)u1\1d\	All	All	All
Operating System	Cisco	Nx-os	5.0\3\	All	All	All
Operating System	Cisco	Nx-os	5.0\3)n1\1c\	All	All	All
Operating System	Cisco	Nx-os	5.0\3)u1\1a\	All	All	All
Operating System	Cisco	Nx-os	5.0\3)u1\1b\	All	All	All
Operating System	Cisco	Nx-os	5.0\3)u1\1d\	All	All	All
Application	Cisco	Nx-os	5.0\2\	All	All	All
Application	Cisco	Nx-os	5.0\3\	All	All	All
Application	Cisco	Nx-os	5.0\3)n1\1a\	All	All	All
Application	Cisco	Nx-os	5.0\3)n1\1b\	All	All	All
Application	Cisco	Nx-os	5.0\3)n1\1c\	All	All	All
Application	Cisco	Nx-os	5.0\3)n1\1\	All	All	All
Application	Cisco	Nx-os	5.0\3)u1\1a\	All	All	All
Application	Cisco	Nx-os	5.0\3)u1\1b\	All	All	All
Application	Cisco	Nx-os	5.0\3)u1\1d\	All	All	All
Application	Cisco	Nx-os	All	All	All	All
Application	Cisco	Nx-os	All	All	All	All
Operating System	Cisco	Nx-os	All	All	All	All

References

Reference	Source
Cisco Nexus Series Switches ACL Deny Statement Security Bypass Security Issue - Secunia.com	SECUNIA
Cisco Security Advisory: Cisco Nexus 5000 and 3000 Series Switches Access Control List Bypass Vulnerability - Cisco Systems	CISCO
Cisco NX-OS Nexus 3000 and 5000 Switches Let Remote Users Bypass Access Control Lists - SecurityTracker	SECTRAC
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](#).

Free CVE JSON API [cve.report/api](#)

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