



CVE-2015-4237

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2015-4237 |
| State | PUBLIC |
| Assigner | psirt@cisco.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2015-07-03 10:59:00 UTC |
| Updated | 2016-12-28 17:07:00 UTC |
| Description | The CLI parser in Cisco NX-OS 4.1(2)E1(1), 6.2(11b), 6.2(12), 7.2(0)ZZ(99.1), 7.2(0)ZZ(99.3), and 9.1(1)SV1(3.1.8) on Ne |

Risk And Classification

Problem Types: CWE-264 | CWE-78

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|----------|--------|-------------|---------|--------|---------|----------|
| Hardware | Cisco | Mds 9100 | - | All | All | All |
| Hardware | Cisco | Mds 9100 | - | All | All | All |
| Hardware | Cisco | Mds 9140 | All | All | All | All |
| Hardware | Cisco | Mds 9140 | All | 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 1000v | - | All | All | All |
| Hardware | Cisco | Nexus 1000v | - | All | All | All |
| Hardware | Cisco | Nexus 3016 | - | All | All | All |
| Hardware | Cisco | Nexus 3016 | - | 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 3132q | - | All | All | All |

| | | | | | | |
|----------|-------|--------------|---|-----|-----|-----|
| Hardware | Cisco | Nexus 3132q | - | All | All | All |
| Hardware | Cisco | Nexus 3164q | - | All | All | All |
| Hardware | Cisco | Nexus 3164q | - | All | All | All |
| Hardware | Cisco | Nexus 3172 | - | All | All | All |
| Hardware | Cisco | Nexus 3172 | - | All | All | All |
| Hardware | Cisco | Nexus 3232c | - | All | All | All |
| Hardware | Cisco | Nexus 3232c | - | 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 4001i | - | All | All | All |
| Hardware | Cisco | Nexus 4001i | - | 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 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 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 93120tx | - | All | All | All |
| Hardware | Cisco | Nexus 93120tx | - | All | All | All |
| Hardware | Cisco | Nexus 93128tx | - | All | All | All |
| Hardware | Cisco | Nexus 93128tx | - | All | All | All |
| Hardware | Cisco | Nexus 9332pq | - | All | All | All |
| Hardware | Cisco | Nexus 9332pq | - | All | All | All |
| Hardware | Cisco | Nexus 9336pq Aci Spine | - | All | All | All |
| Hardware | Cisco | Nexus 9336pq Aci Spine | - | All | All | All |
| Hardware | Cisco | Nexus 9372px | - | All | All | All |
| Hardware | Cisco | Nexus 9372px | - | All | All | All |
| Hardware | Cisco | Nexus 9372tx | - | All | All | All |
| Hardware | Cisco | Nexus 9372tx | - | All | All | All |
| Hardware | Cisco | Nexus 9396px | - | All | All | All |
| Hardware | Cisco | Nexus 9396px | - | All | All | All |
| Hardware | Cisco | Nexus 9396tx | - | All | All | All |
| Hardware | Cisco | Nexus 9396tx | - | 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 | 4.1(2)e1(1) | All | All | All |
| Operating System | Cisco | Nx-os | 4.1(2)e1(1) | All | All | All |
| Operating System | Cisco | Nx-os | 6.2(11b) | All | All | All |
| Operating System | Cisco | Nx-os | 6.2(12) | All | All | All |
| Operating System | Cisco | Nx-os | 6.2(11b) | All | All | All |
| Operating System | Cisco | Nx-os | 6.2(12) | All | All | All |
| Operating System | Cisco | Nx-os | 7.2(0)zz(99.1) | All | All | All |
| Operating System | Cisco | Nx-os | 7.2(0)zz(99.3) | All | All | All |
| Operating System | Cisco | Nx-os | 7.2(0)zz(99.1) | All | All | All |
| Operating System | Cisco | Nx-os | 7.2(0)zz(99.3) | All | All | All |
| Operating System | Cisco | Nx-os | 9.1(1)sv1(3.1.8) | All | All | All |
| Operating System | Cisco | Nx-os | 9.1(1)sv1(3.1.8) | All | All | All |
| Operating System | Cisco | Nx-os | 4.1(2)e1(1) | All | All | All |

| | | | | | | |
|------------------|-------|-------|------------------|-----|-----|-----|
| Operating System | Cisco | Nx-os | 6.2\11b\ | All | All | All |
| Operating System | Cisco | Nx-os | 6.2\12\ | All | All | All |
| Operating System | Cisco | Nx-os | 7.2\0\zz\99.1\ | All | All | All |
| Operating System | Cisco | Nx-os | 7.2\0\zz\99.3\ | All | All | All |
| Operating System | Cisco | Nx-os | 9.1\1\sv1\3.1.8\ | All | All | All |

References

| Reference | Source | Link |
|--|----------|---|
| Cisco Nexus Operating System Devices Command Line Interface Local Privilege Escalation Vulnerability | CISCO | tools.cisco.com |
| Cisco NX-OS Filename Validation Flaw Lets Local Users Gain Elevated Privileges - SecurityTracker | SECTRACK | www.securitytracker.com |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

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). This site includes MITRE data granted under the following [license](https://www.mitre.org).

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