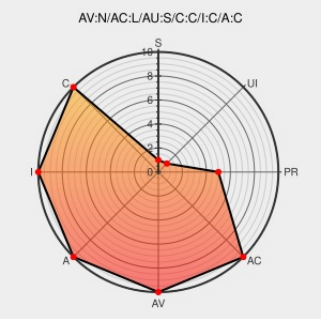
# CVE-2015-4235

Published on: 07/24/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:05 PM UTC

## CVE-2015-4235

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Application Policy Infrastructure Controller Apic from Cisco contain the following vulnerability:

Cisco Application Policy Infrastructure Controller (APIC) devices with software before 1.0(3o) and 1.1 before 1.1(1j) and Nexus 9000 ACI devices with software before 11.0(4o) and 11.1 before 11.1(1j) do not properly restrict access to the APIC filesystem, which allows remote authenticated users to obtain root privileges via unspecified use of the APIC cluster-management configuration feature, aka Bug IDs CSCuu72094 and CSCuv11991.

CVE-2015-4235 has been assigned by psirt@cisco.com to track the vulnerability

### CVSS2 Score: 9 - HIGH

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | SINGLE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| COMPLETE | COMPLETE | COMPLETE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| Cisco NX-OS Application Policy Infrastructure Controller (APIC) Lets Remote Authenticated Users Gain Elevated Privileges - SecurityTracker | www.securitytracker.com text/html | SECTRACK 1033025 |
| Cisco Application Policy Infrastructure Controller Access Control Vulnerability | Vendor Advisory tools.cisco.com text/html | CISCO 20150722 Cisco Application Policy Infrastructure Controller Access Control Vulnerability |

comment@cve.report.

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Cisco | Application Policy Infrastructure Controller Apic | 1.0(1e) | All | All | All |
| Operating System | Cisco | Application Policy Infrastructure Controller Apic | 1.0\(1e\) | All | All | All |
| Operating System | Cisco | Application Policy Infrastructure Controller Apic | 1.0\(1e\) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0(1b) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0(1c) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0(1d) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0(1e) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0(2j) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0(2m) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0(3f) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0(3i) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0(3k) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0(3n) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0(4h) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0\(1b\) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0\(1c\) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0\(1d\) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0\(1e\) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0\(2j\) | All | All | All |
| Operating | Cisco | Nx-os | 11.0\(2m\) | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| System | | | | | | |
| Operating System | Cisco | Nx-os | 11.0\(3f\) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0\(3i\) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0\(3k\) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0\(3n\) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0\(4h\) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0\(1b\) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0\(1c\) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0\(1d\) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0\(1e\) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0\(2j\) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0\(2m\) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0\(3f\) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0\(3i\) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0\(3k\) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0\(3n\) | All | All | All |
| Operating System | Cisco | Nx-os | 11.0\(4h\) | All | All | All |

cpe:2.3:o:cisco:application_policy_infrastructure_controller_(apic):1.0(1e):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:application_policy_infrastructure_controller_\(apic\):1.0\(1e\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:application_policy_infrastructure_controller_\(apic\):1.0\(1e\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0(1b):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0(1c):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0(1d):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0(1e):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0(2j):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0(2m):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0(3f):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0(3i):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0(3k):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0(3n):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0(4h):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\(1b\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\(1c\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\(1d\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\(1e\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\(2j\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\(2m\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\(3f\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\(3i\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\(3k\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\(3n\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\(4h\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\(1b\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\(1c\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\(1d\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\(1e\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\(2j\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\(2m\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\(3f\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\(3i\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\(3k\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\(3n\):*:*:*:*:*:*:*:

cpe:2.3:o:cisco:nx-os:11.0\(4h\):*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→