



CVE-2012-4121

Published on: 10/13/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:14 PM UTC

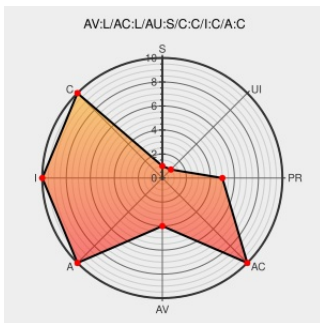
CVE-2012-4121

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Nx-os** from **Cisco** contain the following vulnerability:

Cisco NX-OS allows local users to gain privileges, and read or modify arbitrary files, via the sed (1) r and (2) w commands, aka Bug IDs CSCts56559, CSCts56565, CSCts56570, and CSCts56574.

CVE-2012-4121 has been assigned by psirt@cisco.com to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

SINGLE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Cisco Security Notice: Cisco NX-OS Software Input Validation Vulnerability

[Vendor Advisory](#)
[tools.cisco.com](#)
[text/html](#)

[CISCO 20131004 Cisco NX-OS Software Input Validation Vulnerability](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to 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	Nx-os	-	All	All	All
Operating System	Cisco	Nx-os	-	All	All	All
cpe:2.3:o:cisco:nx-os:-:*****:						
cpe:2.3:o:cisco:nx-os:-:*****:						
No vendor comments have been submitted for this CVE						
← Previous ID				Next ID→		