

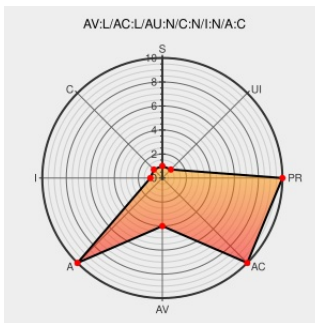


CVE-2015-4277

Published on: 08/19/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:06 PM UTC

CVE-2015-4277

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Nexus 93120tx](#) from [Cisco](#) contain the following vulnerability:

The global-configuration implementation on Cisco ASR 9000 devices with software 5.1.3 and 5.3.0 improperly closes vty sessions after a commit/end operation, which allows local users to cause a denial of service (tmp/*config file creation, memory consumption, and device hang) via unspecified vectors, aka Bug ID CSCut93842.

CVE-2015-4277 has been assigned by [psirt@cisco.com](#) to track the vulnerability

CVSS2 Score: **4.9 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Cisco ASR 9000 Series Router vty Session Closing Bug Lets Local Users Consume Excessive Memory Resources - SecurityTracker

[www.securitytracker.com](#)
[text/html](#)

[SECTrack 1033259](#)

No Description Provided

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

[CISCO 20150811 Cisco ASR 9000 Series Aggregation Services Routers tmp Files Denial of Service 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
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	5.1.3	All	All	All
Operating System	Cisco	Nx-os	5.3.0	All	All	All
Operating System	Cisco	Nx-os	5.1.3	All	All	All
Operating System	Cisco	Nx-os	5.3.0	All	All	All

```
cpe:2.3:h:cisco:nexus_93120tx:-:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:nexus_93120tx:-:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:nexus_93128tx:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:nexus_93128tx:-:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:nexus_9332pq:-:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:nexus_9332pq:-:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:nexus_9336pq_aci_spine:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:nexus_9336pq_aci_spine:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:nexus_9372px:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:nexus_9372px:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:nexus_9372tx:-:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:nexus_9372tx:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:nexus_9396px:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:nexus_9396px:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:nexus_9396tx:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:nexus_9396tx:-:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:nexus_9504:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:nexus 9504:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:nexus_9508:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:nexus_9508:-:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:nexus_9516:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:nexus_9516:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:nx-os:5.1.3:*:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:nx-os:5.3.0:*:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:nx-os:5.1.3:*:*:*:*:*:*:
```

```
cpe:2.3:o:cisco:nx-os:5.3.0:*:*:*:*:*:*:
```

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023   |

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](#).

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