



# CVE-2021-1523

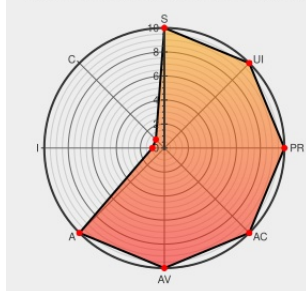
Published on: 08/25/2021 12:00:00 AM UTC

Last Modified on: 09/02/2021 11:22:00 AM UTC

## CVE-2021-1523 - advisory for cisco-sa-n9kaci-queue-wedge-cLDDEfKF

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H



Certain versions of **Nexus 93120tx** from **Cisco** contain the following vulnerability:

A vulnerability in Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) Mode could allow an unauthenticated, remote attacker to cause a queue wedge on a leaf switch, which could result in critical control plane traffic to the device being dropped. This could result in one or more leaf switches being

removed from the fabric. This vulnerability is due to mishandling of ingress TCP traffic to a specific port. An attacker could exploit this vulnerability by sending a stream of TCP packets to a specific port on a Switched Virtual Interface (SVI) configured on the device. A successful exploit could allow the attacker to cause a specific packet queue to queue network buffers but never process them, leading to an eventual queue wedge. This could cause control plane traffic to be dropped, resulting in a denial of service (DoS) condition where the leaf switches are unavailable. Note: This vulnerability requires a manual intervention to power-cycle the device to recover.

CVE-2021-1523 has been assigned by [Cisco](#) psirt@cisco.com to track the vulnerability - currently rated as **HIGH** severity.

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Affected Vendor/Software: [Cisco](#) **Cisco - Cisco NX-OS System Software in ACI Mode** version n/a

CVSS3 Score: **8.6 - HIGH**

| Attack Vector  | Attack Complexity      | Privileges Required | User Interaction    |
|----------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b> | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope          | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>CHANGED</b> | <b>NONE</b>            | <b>NONE</b>         | <b>HIGH</b>         |

CVSS2 Score: **5 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| NETWORK                | LOW               | NONE                |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| NONE                   | NONE              | PARTIAL             |

## CVE References

| Description                                                                                  | Tags                                                         | Link                                                                                                                                                                                                          |
|----------------------------------------------------------------------------------------------|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco Nexus 9000 Series Fabric Switches ACI Mode Queue Wedge Denial of Service Vulnerability | <a href="#">tools.cisco.com</a><br><a href="#">text/html</a> |  <a href="#">CISCO 20210825 Cisco Nexus 9000 Series Fabric Switches ACI Mode Queue Wedge Denial of Service Vulnerability</a> |

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](mailto:comment@cve.report).

## Related QID Numbers

**317021** Cisco Nexus 9000 Series Fabric Switches ACI Mode Queue Wedge Denial of Service Vulnerability (cisco-sa-n9kaci-queue-wedge-clDDEfKF)

## Known Affected Configurations (CPE V2.3)

| Type                                                                                                                                                                             | Vendor | Product        | Version     | Update | Edition | Language |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|----------------|-------------|--------|---------|----------|
| Hardware   | Cisco  | Nexus 93120tx  | -           | All    | All     | All      |
| Hardware   | Cisco  | Nexus 93128tx  | -           | All    | All     | All      |
| Hardware   | Cisco  | Nexus 9332pq   | -           | All    | All     | All      |
| Hardware   | Cisco  | Nexus 9372px   | -           | All    | All     | All      |
| Hardware   | Cisco  | Nexus 9372px-e | -           | All    | All     | All      |
| Hardware   | Cisco  | Nexus 9372tx   | -           | All    | All     | All      |
| Hardware   | Cisco  | Nexus 9372tx-e | -           | All    | All     | All      |
| Hardware   | Cisco  | Nexus 9396px   | -           | All    | All     | All      |
| Hardware   | Cisco  | Nexus 9396tx   | -           | All    | All     | All      |
| Operating System                                                                                                                                                                 | Cisco  | Nx-os          | 13.2\ (3n\) | All    | All     | All      |
| Operating System                                                                                                                                                                 | Cisco  | Nx-os          | 14.2\ (4i\) | All    | All     | All      |

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

```
cpe:2.3:h:cisco:nexus 93128tx:-:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:nexus 9332pq:-:*:*:*:*:*:
```

|                                             |
|---------------------------------------------|
| cpe:2.3:h:cisco:nexus_9372px:-:*:*:*:*:*:   |
| cpe:2.3:h:cisco:nexus_9372px-e:-:*:*:*:*:*: |
| cpe:2.3:h:cisco:nexus_9372tx:-:*:*:*:*:*:   |
| cpe:2.3:h:cisco:nexus_9372tx-e:-:*:*:*:*:*: |
| cpe:2.3:h:cisco:nexus_9396px:-:*:*:*:*:*:   |
| cpe:2.3:h:cisco:nexus_9396tx:-:*:*:*:*:*:   |
| cpe:2.3:o:cisco:nx-os:13.2(3n\):*:*:*:*:*:  |
| cpe:2.3:o:cisco:nx-os:14.2(4i\):*:*:*:*:*:  |

No vendor comments have been submitted for this CVE

## Social Mentions

| Source                                                                                              | Title                                                                                                                                                                                                                | Posted (UTC)        |
|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
|  @CVEreport         | CVE-2021-1523 : A vulnerability in Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure... <a href="https://twitter.com/i/web/status/1461811111111111111">twitter.com/i/web/status/1...</a> | 2021-08-25 19:20:30 |
|  @LinInfoSec      | Nexus - CVE-2021-1523: <a href="https://tools.cisco.com/security/center/content/CiscoSecurityCenter#CVE-2021-1523">tools.cisco.com/security/cente...</a>                                                             | 2021-08-25 20:36:32 |
| <br>@RedPacketSec | CVE-2021-1523 - <a href="https://redpacketsecurity.com/cve-2021-1523/">redpacketsecurity.com/cve-2021-1523/</a> #cybersecurity                                                                                       | 2021-09-02 14:51:05 |
| <br>@RedPacketSec | CVE-2021-1523 - <a href="https://redpacketsecurity.com/cve-2021-1523-...">redpacketsecurity.com/cve-2021-1523-...</a> #cybersecurity                                                                                 | 2021-09-02 14:51:16 |

[← Previous ID](#)

Next ID→

© 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](https://status.cve.report)