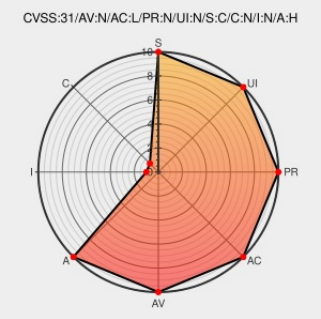
CVE-2021-1523

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



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 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 NX-OS System Software in ACI Mode** version **n/a**

CVSS3 Score: 8.6 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	NONE	NONE	HIGH

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	tools.cisco.com text/html	CISCO 20210825 Cisco Nexus 9000 Series Fabric Switches ACI Mode Queue Wedge Denial of Service Vulnerability

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… twitter.com/i/web/status/1…	2021-08-25 19:20:30
@LinInfoSec	Nexus - CVE-2021-1523: tools.cisco.com/security/cente…	2021-08-25 20:36:32
@RedPacketSec	CVE-2021-1523 - redpacketsecurity.com/cve-2021-1523/ #cybersecurity	2021-09-02 14:51:05
@RedPacketSec	CVE-2021-1523 - redpacketsecurity.com/cve-2021-1523-… #cybersecurity	2021-09-02 14:51:16

← Previous ID

Next ID→