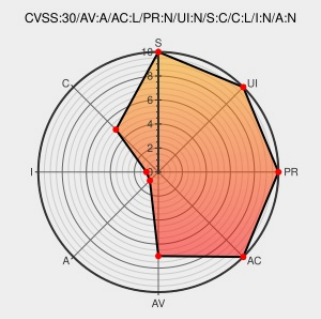
CVE-2020-3231

Published on: 06/03/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:38 PM UTC

CVE-2020-3231 - advisory for cisco-sa-c2960L-DpWA9Re4

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



Certain versions of Ios from Cisco contain the following vulnerability:

A vulnerability in the 802.1X feature of Cisco Catalyst 2960-L Series Switches and Cisco Catalyst CDB-8P Switches could allow an unauthenticated, adjacent attacker to forward broadcast traffic before being authenticated on the port. The vulnerability exists because broadcast traffic that is received on the 802.1X-enabled port is mishandled. An attacker could exploit this vulnerability by sending broadcast traffic on the port before being authenticated. A successful exploit could allow the attacker to send and receive broadcast traffic on the 802.1X-enabled port before authentication.

CVE-2020-3231 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as MEDIUM 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 IOS 15.2(5a)E** version **n/a**

CVSS3 Score: 4.7 - MEDIUM

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

CVSS2 Score: 2.9 - LOW

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

PARTIAL | NONE | NONE

CVE References

Description	Tags	Link
Cisco IOS Software for Catalyst 2960-L Series Switches and Catalyst CDB-8P Switches 802.1X Authentication Bypass Vulnerability	Patch Vendor Advisory tools.cisco.com text/html	CISCO 20200603 Cisco IOS Software for Catalyst 2960-L Series Switches and Catalyst CDB-8P Switches 802.1X Authentication Bypass Vulnerability

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	Ios	15.2\(5a\)e	All	All	All
Operating System	Cisco	Ios	15.2\(5b\)e	All	All	All
Operating System	Cisco	Ios	15.2\(5c\)e	All	All	All
Operating System	Cisco	Ios	15.2\(5\)e2	All	All	All
Operating System	Cisco	Ios	15.2\(5\)ex	All	All	All
Operating System	Cisco	Ios	15.2\(6\)e	All	All	All
Operating System	Cisco	Ios	15.2\(6\)e0c	All	All	All
Operating System	Cisco	Ios	15.2\(6\)e1	All	All	All
Operating System	Cisco	Ios	15.2\(6\)e1a	All	All	All
Operating System	Cisco	Ios	15.2\(6\)e1s	All	All	All
Operating System	Cisco	Ios	15.2\(6\)e2	All	All	All
Operating System	Cisco	Ios	15.2\(6\)e2b	All	All	All
Operating System	Cisco	Ios	15.2\(6\)e3	All	All	All
Operating System	Cisco	Ios	15.2\(6\)e4	All	All	All

Operating System	Cisco	Ios	15.2\(7a\)e0b	All	All	All
Operating System	Cisco	Ios	15.2\(7b\)e0b	All	All	All
Operating System	Cisco	Ios	15.2\(7\)e	All	All	All
Operating System	Cisco	Ios	15.2\(7\)e0a	All	All	All
Operating System	Cisco	Ios	15.2\(7\)e0b	All	All	All
Operating System	Cisco	Ios	15.2\(7\)e0s	All	All	All
Operating System	Cisco	Ios	15.3\(3\)jaa1	All	All	All
Operating System	Cisco	Ios	15.3\(3\)jpj	All	All	All
Operating System	Cisco	Ios	15.2\(5a\)e	All	All	All
Operating System	Cisco	Ios	15.2\(5b\)e	All	All	All
Operating System	Cisco	Ios	15.2\(5c\)e	All	All	All
Operating System	Cisco	Ios	15.2\(5\)e2	All	All	All
Operating System	Cisco	Ios	15.2\(5\)ex	All	All	All
Operating System	Cisco	Ios	15.2\(6\)e	All	All	All
Operating System	Cisco	Ios	15.2\(6\)e0c	All	All	All
Operating System	Cisco	Ios	15.2\(6\)e1	All	All	All
Operating System	Cisco	Ios	15.2\(6\)e1a	All	All	All
Operating System	Cisco	Ios	15.2\(6\)e1s	All	All	All
Operating System	Cisco	Ios	15.2\(6\)e2	All	All	All
Operating System	Cisco	Ios	15.2\(6\)e2b	All	All	All
Operating System	Cisco	Ios	15.2\(6\)e3	All	All	All
Operating System	Cisco	Ios	15.2\(6\)e4	All	All	All
Operating System	Cisco	Ios	15.2\(7a\)e0b	All	All	All

Operating System	Cisco	Ios	15.2\(7b\)e0b	All	All	All
Operating System	Cisco	Ios	15.2\(7\)e	All	All	All
Operating System	Cisco	Ios	15.2\(7\)e0a	All	All	All
Operating System	Cisco	Ios	15.2\(7\)e0b	All	All	All
Operating System	Cisco	Ios	15.2\(7\)e0s	All	All	All
Operating System	Cisco	Ios	15.3\(3\)jaa1	All	All	All
Operating System	Cisco	Ios	15.3\(3\)jpj	All	All	All

cpe:2.3:o:cisco:ios:15.2\(5a\)e:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(5b\)e:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(5c\)e:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(5\)e2:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(5\)ex:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(6\)e:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(6\)e0c:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(6\)e1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(6\)e1a:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(6\)e1s:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(6\)e2:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(6\)e2b:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(6\)e3:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(6\)e4:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(7a\)e0b:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(7b\)e0b:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(7\)e:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(7\)e0a:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(7\)e0b:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(7\)e0s:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.3\(3\)jaa1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.3\(3\)jpj:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(5a\)e:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(5b\)e:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(5c\)e:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(5\)e2:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(5\)ex:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(6\)e:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(6\)e0c:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(6\)e1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(6\)e1a:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(6\)e1s:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(6\)e2:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(6\)e2b:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(6\)e3:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(6\)e4:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(7a\)e0b:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(7b\)e0b:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(7\)e:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(7\)e0a:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(7\)e0b:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.2\(7\)e0s:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.3\(3\)jaa1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios:15.3\(3\)jpj:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report