

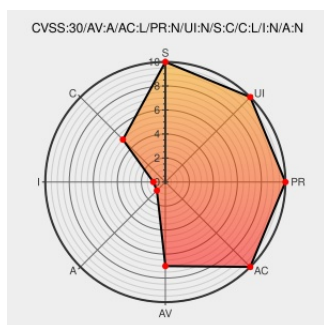


CVE-2020-3231

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

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

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	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	los	15.2\7a\0b	All	All	All
Operating System	Cisco	los	15.2\7b\0b	All	All	All
Operating System	Cisco	los	15.2\7\0e	All	All	All
Operating System	Cisco	los	15.2\7\0a	All	All	All
Operating System	Cisco	los	15.2\7\0b	All	All	All
Operating System	Cisco	los	15.2\7\0s	All	All	All
Operating System	Cisco	los	15.3\3\jaa1	All	All	All
Operating System	Cisco	los	15.3\3\jppj	All	All	All
Operating System	Cisco	los	15.2\5a\0e	All	All	All
Operating System	Cisco	los	15.2\5b\0e	All	All	All
Operating System	Cisco	los	15.2\5c\0e	All	All	All
Operating System	Cisco	los	15.2\5\0e2	All	All	All
Operating System	Cisco	los	15.2\5\0ex	All	All	All
Operating System	Cisco	los	15.2\6\0e	All	All	All
Operating System	Cisco	los	15.2\6\0c	All	All	All
Operating System	Cisco	los	15.2\6\0e1	All	All	All
Operating System	Cisco	los	15.2\6\0e1a	All	All	All
Operating System	Cisco	los	15.2\6\0e1s	All	All	All
Operating System	Cisco	los	15.2\6\0e2	All	All	All
Operating System	Cisco	los	15.2\6\0e2b	All	All	All
Operating System	Cisco	los	15.2\6\0e3	All	All	All
Operating System	Cisco	los	15.2\6\0e4	All	All	All
Operating System	Cisco	los	15.2\7a\0b	All	All	All

Operating System	Cisco	ios	15.2\7b\0b	All	All	All
Operating System	Cisco	ios	15.2\7\0e	All	All	All
Operating System	Cisco	ios	15.2\7\0a	All	All	All
Operating System	Cisco	ios	15.2\7\0b	All	All	All
Operating System	Cisco	ios	15.2\7\0s	All	All	All
Operating System	Cisco	ios	15.3\3\jaa1	All	All	All
Operating System	Cisco	ios	15.3\3\jpi	All	All	All
cpe:2.3:o:cisco:ios:15.2\5a\0e:*****:						
cpe:2.3:o:cisco:ios:15.2\5b\0e:*****:						
cpe:2.3:o:cisco:ios:15.2\5c\0e:*****:						
cpe:2.3:o:cisco:ios:15.2\5\0e2:*****:						
cpe:2.3:o:cisco:ios:15.2\5\0ex:*****:						
cpe:2.3:o:cisco:ios:15.2\6\0e:*****:						
cpe:2.3:o:cisco:ios:15.2\6\0c:*****:						
cpe:2.3:o:cisco:ios:15.2\6\0e1:*****:						
cpe:2.3:o:cisco:ios:15.2\6\0e1a:*****:						
cpe:2.3:o:cisco:ios:15.2\6\0e1s:*****:						
cpe:2.3:o:cisco:ios:15.2\6\0e2:*****:						
cpe:2.3:o:cisco:ios:15.2\6\0e2b:*****:						
cpe:2.3:o:cisco:ios:15.2\6\0e3:*****:						
cpe:2.3:o:cisco:ios:15.2\6\0e4:*****:						
cpe:2.3:o:cisco:ios:15.2\7a\0b:*****:						
cpe:2.3:o:cisco:ios:15.2\7b\0b:*****:						
cpe:2.3:o:cisco:ios:15.2\7\0e:*****:						
cpe:2.3:o:cisco:ios:15.2\7\0a:*****:						
cpe:2.3:o:cisco:ios:15.2\7\0b:*****:						
cpe:2.3:o:cisco:ios:15.2\7\0s:*****:						

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](#) 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](#)