



CVE-2016-1399

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2016-1399
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-05-14 01:59:00 UTC
Updated	2021-10-06 17:09:00 UTC
Description	The packet-processing microcode in Cisco IOS 15.2(2)EA, 15.2(2)EA1, 15.2(2)EA2, and 15.2(4)EA on Industrial Ethernet 4

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	le-4000-16gt4g-e	-	All	All	All
Hardware	Cisco	le-4000-16gt4g-e	-	All	All	All
Hardware	Cisco	le-4000-16t4g-e	-	All	All	All
Hardware	Cisco	le-4000-16t4g-e	-	All	All	All
Hardware	Cisco	le-4000-4gc4gp4g-e	-	All	All	All
Hardware	Cisco	le-4000-4gc4gp4g-e	-	All	All	All
Hardware	Cisco	le-4000-4gs8gp4g-e	-	All	All	All
Hardware	Cisco	le-4000-4gs8gp4g-e	-	All	All	All
Hardware	Cisco	le-4000-4s8p4g-e	-	All	All	All
Hardware	Cisco	le-4000-4s8p4g-e	-	All	All	All
Hardware	Cisco	le-4000-4t4p4g-e	-	All	All	All
Hardware	Cisco	le-4000-4t4p4g-e	-	All	All	All
Hardware	Cisco	le-4000-4tc4g-e	-	All	All	All
Hardware	Cisco	le-4000-4tc4g-e	-	All	All	All
Hardware	Cisco	le-4000-8gs4g-e	-	All	All	All
Hardware	Cisco	le-4000-8gs4g-e	-	All	All	All
Hardware	Cisco	le-4000-8gt4g-e	-	All	All	All

Hardware	Cisco	le-4000-8gt4g-e	-	All	All	All
Hardware	Cisco	le-4000-8gt8gp4g-e	-	All	All	All
Hardware	Cisco	le-4000-8gt8gp4g-e	-	All	All	All
Hardware	Cisco	le-4000-8s4g-e	-	All	All	All
Hardware	Cisco	le-4000-8s4g-e	-	All	All	All
Hardware	Cisco	le-4000-8t4g-e	-	All	All	All
Hardware	Cisco	le-4000-8t4g-e	-	All	All	All
Hardware	Cisco	le-5000-12s12p-10g	-	All	All	All
Hardware	Cisco	le-5000-12s12p-10g	-	All	All	All
Hardware	Cisco	le-5000-16s12p	-	All	All	All
Hardware	Cisco	le-5000-16s12p	-	All	All	All
Application	Cisco	los	15.2(2)ea	All	All	All
Application	Cisco	los	15.2(2)ea1	All	All	All
Application	Cisco	los	15.2(2)ea2	All	All	All
Application	Cisco	los	15.2(2)eb	All	All	All
Application	Cisco	los	15.2(2)eb1	All	All	All
Application	Cisco	los	15.2(4)ea	All	All	All
Application	Cisco	los	15.2(2)ea	All	All	All
Application	Cisco	los	15.2(2)ea1	All	All	All
Application	Cisco	los	15.2(2)ea2	All	All	All
Application	Cisco	los	15.2(2)eb	All	All	All
Application	Cisco	los	15.2(2)eb1	All	All	All
Application	Cisco	los	15.2(4)ea	All	All	All
Operating System	Cisco	los	15.2(2)ea	All	All	All
Operating System	Cisco	los	15.2(2)ea1	All	All	All
Operating System	Cisco	los	15.2(2)eb	All	All	All
Operating System	Cisco	los	15.2(2)eb1	All	All	All
Application	Cisco	los	15.2(2)ea	All	All	All
Application	Cisco	los	15.2(2)ea1	All	All	All
Application	Cisco	los	15.2(2)ea2	All	All	All
Application	Cisco	los	15.2(2)eb	All	All	All
Application	Cisco	los	15.2(2)eb1	All	All	All
Application	Cisco	los	15.2(4)ea	All	All	All

References

Reference

Cisco Industrial Ethernet Switch Packet Processing Flaw Lets Remote Users Corrupt Queued Data on the Target System - SecurityTracker

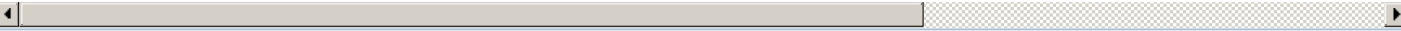
Cisco Industrial Ethernet 4000 and 5000 Series Switches Remote Security Bypass Vulnerability

Rockwell Automation Allen-Bradley Stratix 5400 and 5410 Packet Corruption Vulnerability | ICS-CERT

Cisco Industrial Ethernet 4000 and Ethernet 5000 Series Switches ICMP IPv4 Packet Corruption Vulnerability

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[590335](#) Rockwell Automation Allen-Bradley Stratix 5400 and 5410 Packet Corruption Vulnerability Vulnerability (ICSA-16-175-01)

© [CVE.report](#) 2026 |

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](#)