



CVE-2018-0175

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

Summary

CVE	CVE-2018-0175
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-28 22:29:00 UTC
Updated	2019-10-09 23:31:00 UTC
Description	Format String vulnerability in the Link Layer Discovery Protocol (LLDP) subsystem of Cisco IOS Software, Cisco IOS XE Sc

Risk And Classification

EPSS: 0.029240000 probability, percentile 0.863500000 (date 2026-04-02)

CISA KEV: Listed on 2022-03-03; due 2022-03-17; ransomware use Unknown

Problem Types: CWE-134

CISA Known Exploited Vulnerability

Vendor	Cisco
Product	IOS, XR, and XE Software
Name	Cisco IOS, XR, and XE Software Buffer Overflow Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2018-0175

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	ios	15.4(3)m4.1	All	All	All
Operating System	Cisco	ios	15.4\{(3)\}m4.1	All	All	All
Operating System	Cisco	ios	15.4\{(3)\}m4.1	All	All	All
Operating System	Cisco	ios Xe	15.4(3)m4.1	All	All	All
Operating System	Cisco	ios Xe	15.4\{(3)\}m4.1	All	All	All
Operating System	Cisco	ios Xe	15.4\{(3)\}m4.1	All	All	All
Operating System	Cisco	ios Xr	15.4(3)m4.1	All	All	All
Operating System	Cisco	ios Xr	15.4\{(3)\}m4.1	All	All	All

Operating System	Cisco	Ios Xr	15.4\3\m4.1	All	All	All
Hardware	Rockwellautomation	Allen-bradley Armorstratix 5700	-	All	All	All
Hardware	Rockwellautomation	Allen-bradley Armorstratix 5700	-	All	All	All
Hardware	Rockwellautomation	Allen-bradley Stratix 5400	-	All	All	All
Hardware	Rockwellautomation	Allen-bradley Stratix 5400	-	All	All	All
Hardware	Rockwellautomation	Allen-bradley Stratix 5410	-	All	All	All
Hardware	Rockwellautomation	Allen-bradley Stratix 5410	-	All	All	All
Hardware	Rockwellautomation	Allen-bradley Stratix 5700	-	All	All	All
Hardware	Rockwellautomation	Allen-bradley Stratix 5700	-	All	All	All
Hardware	Rockwellautomation	Allen-bradley Stratix 5900 Services Router	-	All	All	All
Hardware	Rockwellautomation	Allen-bradley Stratix 5900 Services Router	-	All	All	All
Hardware	Rockwellautomation	Allen-bradley Stratix 8000	-	All	All	All
Hardware	Rockwellautomation	Allen-bradley Stratix 8000	-	All	All	All

References

Reference

Cisco IOS, IOS XE, and IOS XR Software Link Layer Discovery Protocol Buffer Overflow Vulnerabilities

Rockwell Automation Stratix and ArmorStratix Switches | CISA

Cisco IOS/IOS XE/IOS XR Software Multiple Remote Code Execution and Format String Vulnerabilities

Rockwell Automation Stratix Industrial Managed Ethernet Switch | ICS-CERT

Cisco IOS/IOS XE/IOS XR Link Layer Discovery Protocol Bugs Let Remote Users on the Local Network Gain Elevated Privileges - SecurityTrails

Rockwell Automation Stratix Services Router | CISA

CVE Program record

NVD vulnerability detail

CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[590338](#) Rockwell Automation Stratix and ArmorStratix Switches Multiple Vulnerabilities (ICSA-18-107-04)

[590339](#) Rockwell Automation Stratix Industrial Managed Ethernet Switch Multiple Vulnerabilities (ICSA-18-107-05)

[590343](#) Rockwell Automation Stratix Services Router Multiple Vulnerabilities (ICSA-18-107-03)

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](#)