



# CVE-2018-0173

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2018-0173
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-03-28 22:29:00 UTC
<b>Updated</b>	2019-10-09 23:31:00 UTC
<b>Description</b>	A vulnerability in the Cisco IOS Software and Cisco IOS XE Software function that restores encapsulated option 82 informa

## Risk And Classification

**EPSS:** 0.054250000 probability, percentile 0.901200000 (date 2026-04-02)

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

**Problem Types:** CWE-20

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Cisco
<b>Product</b>	IOS and IOS XE Software
<b>Name</b>	Cisco IOS and IOS XE Software Improper Input Validation Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2018-0173">https://nvd.nist.gov/vuln/detail/CVE-2018-0173</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Cisco</a>	<a href="#">4321 Integrated Services Router</a>	-	All	All	All
Hardware	<a href="#">Cisco</a>	<a href="#">4321 Integrated Services Router</a>	-	All	All	All
Hardware	<a href="#">Cisco</a>	<a href="#">4331 Integrated Services Router</a>	-	All	All	All
Hardware	<a href="#">Cisco</a>	<a href="#">4331 Integrated Services Router</a>	-	All	All	All
Hardware	<a href="#">Cisco</a>	<a href="#">4351 Integrated Services Router</a>	-	All	All	All
Hardware	<a href="#">Cisco</a>	<a href="#">4351 Integrated Services Router</a>	-	All	All	All
Hardware	<a href="#">Cisco</a>	<a href="#">4431 Integrated Services Router</a>	-	All	All	All
Hardware	<a href="#">Cisco</a>	<a href="#">4431 Integrated Services Router</a>	-	All	All	All

Hardware	Cisco	4451-x Integrated Services Router	-	All	All	All
Hardware	Cisco	4451-x Integrated Services Router	-	All	All	All
Hardware	Cisco	Asr 1000 Series Route Processor Rp2	-	All	All	All
Hardware	Cisco	Asr 1000 Series Route Processor Rp3	-	All	All	All
Hardware	Cisco	Asr 1000 Series Route Processor Rp2	-	All	All	All
Hardware	Cisco	Asr 1000 Series Route Processor Rp2	-	All	All	All
Hardware	Cisco	Asr 1000 Series Route Processor Rp3	-	All	All	All
Hardware	Cisco	Asr 1000 Series Route Processor Rp3	-	All	All	All
Hardware	Cisco	Asr 1001-hx	-	All	All	All
Hardware	Cisco	Asr 1001-hx	-	All	All	All
Hardware	Cisco	Asr 1001-x	-	All	All	All
Hardware	Cisco	Asr 1001-x	-	All	All	All
Hardware	Cisco	Asr 1002-hx	-	All	All	All
Hardware	Cisco	Asr 1002-hx	-	All	All	All
Hardware	Cisco	Asr 1002-x	-	All	All	All
Hardware	Cisco	Asr 1002-x	-	All	All	All
Hardware	Cisco	Cloud Services Router 1000v	-	All	All	All
Hardware	Cisco	Cloud Services Router 1000v	-	All	All	All
Operating System	Cisco	ios	denali-16.3.4	All	All	All
Operating System	Cisco	ios	denali-16.3.4	All	All	All
Operating System	Cisco	ios Xe	denali-16.3.4	All	All	All
Operating System	Cisco	ios Xe	denali-16.3.4	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 8000	-	All	All	All
Hardware	Rockwellautomation	Allen-bradley Stratix 8000	-	All	All	All
Hardware	Rockwellautomation	Allen-bradley Stratix 8300	-	All	All	All
Hardware	Rockwellautomation	Allen-bradley Stratix 8300	-	All	All	All

## References

Reference	Source
Rockwell Automation Stratix and ArmorStratix Switches   CISA	MISC
Rockwell Automation Stratix Industrial Managed Ethernet Switch   ICS-CERT	MISC
Cisco IOS/IOS XE DHCP Option 82 Processing Bugs Let Remote Users Cause the Target System to Reload - SecurityTracker	SECTRACK
Cisco IOS and IOS XE Software DHCP Version 4 Relay Reply Denial of Service Vulnerability	CONFIRM
Cisco IOS and IOS XE Software CVE-2018-0173 Denial of Service Vulnerability	BID
[R1] Cisco IOS and IOS XE Multiple Memory Corruption Vulnerabilities - Research Advisory   Tenable®	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
CISA Known Exploited Vulnerabilities catalog	CISA

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)

© [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](#)