



# CVE-2017-12235

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

## Summary

<b>CVE</b>	CVE-2017-12235
<b>State</b>	PUBLISHED
<b>Assigner</b>	cisco
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-09-29 01:34:48 UTC
<b>Updated</b>	2026-04-21 18:08:19 UTC
<b>Description</b>	A vulnerability in the implementation of the PROFINET Discovery and Configuration Protocol (PN-DCP) for Cisco IOS 12.2

## Risk And Classification

**Primary CVSS:** v3.1 7.5 HIGH from nvd@nist.gov

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

**EPSS:** 0.065450000 probability, percentile 0.911760000 (date 2026-04-25)

**CISA KEV:** Listed on 2022-03-03; due 2022-03-24; ransomware use Unknown

**Problem Types:** CWE-20 | NVD-CWE-noinfo | CWE-20 CWE-20

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	ADP	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
2.0	nvd@nist.gov	Primary	7.8		AV:N/AC:L/Au:N/C:N/I:N/A:C

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

### CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

AV:N/AC:L/Au:N/C:N/I:N/A:C

### CISA Known Exploited Vulnerability

<b>Vendor</b>	Cisco
<b>Product</b>	IOS software
<b>Name</b>	Cisco IOS Software for Cisco Industrial Ethernet Switches PROFINET Denial-of-Service Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2017-12235">https://nvd.nist.gov/vuln/detail/CVE-2017-12235</a>

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Industrial Ethernet 2000 16ptc-g-e Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 16ptc-g-l Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 16ptc-g-nx Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 16t67-b Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 16t67p-g-e Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 16tc-g-e Switch	-	All	All	All

Hardware	Cisco	Industrial Ethernet 2000 16tc-g-l Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 16tc-g-n Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 16tc-g-x Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 16tc-l Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 24t67-b Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 4s-ts-g-b Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 4s-ts-g-l Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 4t-b Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 4t-g-b Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 4t-g-l Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 4t-l Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 4ts-b Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 4ts-g-b Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 4ts-g-l Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 4ts-l Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 8t67-b Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 8t67p-g-e Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 8tc-b Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 8tc-g-b Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 8tc-g-e Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 8tc-g-l Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 8tc-g-n Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 8tc-l Switch	-	All	All	All
Hardware	Cisco	Industrial Ethernet 2000 Series Firmware	15.2(5.4.32i)e2	All	All	All
Operating System	Cisco	ios	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	Cisco IOS	affected Cisco IOS	Not specified

### References

#### Reference

Malformed Request

[www.cisa.gov/known-exploited-vulnerabilities-catalog](http://www.cisa.gov/known-exploited-vulnerabilities-catalog)

Cisco Industrial Ethernet Switch PROFINET PN-DCP Packet Parsing Bug Lets Remote Users Cause the Target System to Reload - SecurityT

Cisco IOS Software for Cisco Industrial Ethernet Switches PROFINET Denial of Service Vulnerability

CVE Program record

NVD vulnerability detail

CISA Known Exploited Vulnerabilities catalog



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)