



# CVE-2017-12238

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

## Summary

<b>CVE</b>	CVE-2017-12238
<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 18:08:05 UTC
<b>Description</b>	A vulnerability in the Virtual Private LAN Service (VPLS) code of Cisco IOS 15.0 through 15.4 for Cisco Catalyst 6800 Serie

## Risk And Classification

**Primary CVSS:** v3.1 6.5 MEDIUM from nvd@nist.gov

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

**EPSS:** 0.010140000 probability, percentile 0.771950000 (date 2026-04-22)

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

**Problem Types:** CWE-399 | NVD-CWE-noinfo | CWE-399 CWE-399

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.5	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	ADP	DECLARED	6.5	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.5	MEDIUM	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
2.0	nvd@nist.gov	Primary	3.3		AV:A/AC:L/Au:N/C:N/I:N/A:P

## CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

### CVSS v2.0 Breakdown

Access Vector

Adjacent

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

### CISA Known Exploited Vulnerability

<b>Vendor</b>	Cisco
<b>Product</b>	Catalyst 6800 Series Switches
<b>Name</b>	Cisco Catalyst 6800 Series Switches VPLS 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-2017-12238">https://nvd.nist.gov/vuln/detail/CVE-2017-12238</a>

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	C6800-16p10g	-	All	All	All
Hardware	Cisco	C6800-16p10g-xl	-	All	All	All
Hardware	Cisco	Catalyst 6000	-	All	All	All
Hardware	Cisco	Catalyst 6000 Ws-svc-nam-1	2.2\1a	All	All	All
Hardware	Cisco	Catalyst 6000 Ws-svc-nam-1	3.1\1a	All	All	All
Hardware	Cisco	Catalyst 6000 Ws-svc-nam-2	2.2\1a	All	All	All

Hardware	Cisco	Catalyst 6000 Ws-svc-nam-2	3.1\1a	All	All	All
Hardware	Cisco	Catalyst 6000 Ws-x6380-nam	2.1\2	All	All	All
Hardware	Cisco	Catalyst 6000 Ws-x6380-nam	3.1\1a	All	All	All
Hardware	Cisco	Catalyst 6500	-	All	All	All
Hardware	Cisco	Catalyst 6500-e	-	All	All	All
Hardware	Cisco	Catalyst 6500 Ws-svc-nam-1	2.2\1a	All	All	All
Hardware	Cisco	Catalyst 6500 Ws-svc-nam-1	3.1\1a	All	All	All
Hardware	Cisco	Catalyst 6500 Ws-svc-nam-2	2.2\1a	All	All	All
Hardware	Cisco	Catalyst 6500 Ws-svc-nam-2	3.1\1a	All	All	All
Hardware	Cisco	Catalyst 6500 Ws-x6380-nam	2.1\2	All	All	All
Hardware	Cisco	Catalyst 6500 Ws-x6380-nam	3.1\1a	All	All	All
Hardware	Cisco	Catalyst 6503-e	-	All	All	All
Hardware	Cisco	Catalyst 6504-e	-	All	All	All
Hardware	Cisco	Catalyst 6506-e	-	All	All	All
Hardware	Cisco	Catalyst 6509-e	-	All	All	All
Hardware	Cisco	Catalyst 6509-neb-a	-	All	All	All
Hardware	Cisco	Catalyst 6509-v-e	-	All	All	All
Hardware	Cisco	Catalyst 6513	-	All	All	All
Hardware	Cisco	Catalyst 6513-e	-	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
<a href="http://www.cisa.gov/known-exploited-vulnerabilities-catalog">www.cisa.gov/known-exploited-vulnerabilities-catalog</a>
Malformed Request
Cisco IOS Software for Cisco Catalyst 6800 Series Switches VPLS Denial of Service Vulnerability
Cisco IOS on Cisco Catalyst 6800 Series Switch VPLS Memory Management Flaw Lets Remote Users Cause the Target Line Card to Crash -
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](#)