



# CVE-2017-12213

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-12213
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-09-07 21:29:00 UTC
<b>Updated</b>	2019-10-09 23:22:00 UTC
<b>Description</b>	A vulnerability in the dynamic access control list (ACL) feature of Cisco IOS XE Software running on Cisco Catalyst 4000 S

## Risk And Classification

**Problem Types:** CWE-287

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Catalyst 4000	-	All	All	All
Hardware	Cisco	Catalyst 4000	-	All	All	All
Operating System	Cisco	ios Xe	-	All	All	All
Operating System	Cisco	ios Xe	-	All	All	All

## References

### Reference

Cisco Catalyst 4000 Series Switch Dynamic ACL Bug Lets Remote Users Bypass Port Access Controls on the Target System - SecurityTrackr
Cisco Catalyst 4000 Series Switches CVE-2017-12213 Authentication Bypass Vulnerability
Cisco Catalyst 4000 Series Switches Dynamic ACL Bypass Vulnerability
CVE Program record
NVD vulnerability detail

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](#).

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