CVE-2017-12213

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-12213
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-07 21:29:00 UTC
Updated	2019-10-09 23:22:00 UTC
Description	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 - SecurityTrack
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.