CVE-2014-8023

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2014-8023
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-02-17 01:59:00 UTC
Updated	2017-09-08 01:29:00 UTC
Description	Cisco Adaptive Security Appliance (ASA) Software 9.2(.3) and earlier, when challenge-response authentication is used, doe

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Adaptive Security Appliance Software	All	All	All	All

References

Reference	Source	
Cisco Adaptive Security Appliance (ASA) Software CVE-2014-8023 Remote Security Bypass Vulnerability	BID	
tools.cisco.com/security/center/viewAlert.x	CONFIRM	
IBM X-Force Exchange	XF	
Cisco ASA VPN Tunnel Group Selection Flaw Lets Remote Authenticated Users Bypass Access Controls - SecurityTracker	SECTRACK	
20150216 Cisco ASA Challenge-Response Tunnel Group Selection Bypass Vulnerability	CISCO	
CVE Program record	CVE.ORG	
NVD vulnerability detail	NVD	

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report