CVE-2001-0929

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

Summary

CVE	CVE-2001-0929
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2001-11-28 05:00:00 UTC
Updated	2017-10-10 01:29:00 UTC
Description	Cisco IOS Firewall Feature set, aka Context Based Access Control (CBAC) or Cisco Secure Integrated Software, for IOS 1

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Ios	11.2p	All	All	All
Operating System	Cisco	Ios	11.3t	All	All	All
Operating System	Cisco	Ios	12.0	All	All	All
Operating System	Cisco	Ios	12.0t	All	All	All
Operating System	Cisco	Ios	12.1	All	All	All
Operating System	Cisco	Ios	12.1e	All	All	All
Operating System	Cisco	Ios	12.1t	All	All	All
Operating System	Cisco	Ios	12.2	All	All	All
Operating System	Cisco	Ios	12.2t	All	All	All
Operating System	Cisco	Ios	11.2p	All	All	All
Operating System	Cisco	Ios	11.3t	All	All	All
Operating System	Cisco	Ios	12.0	All	All	All
Operating System	Cisco	Ios	12.0t	All	All	All
Operating System	Cisco	Ios	12.1	All	All	All
Operating System	Cisco	Ios	12.1e	All	All	All
Operating System	Cisco	Ios	12.1t	All	All	All
Operating System	Cisco	Ios	12.2	All	All	All

Operating System	Cisco	Ios	12.2t	All	All	All

References

Reference	Source	Link	Tags
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
Cisco - Networking, Cloud, and Cybersecurity Solutions	CISCO	www.cisco.com	Patch, Vendor
404 Not Found	OSVDB	www.osvdb.org	
Cisco Context Based Access Control Protocol Check Bypassing Vulnerability	BID	www.securityfocus.com	
CERT/CC Vulnerability Note VU#362483	CERT-VN	www.kb.cert.org	US Governmer
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

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