CVE-2006-0764

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2006-0764
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-02-18 02:02:00 UTC
Updated	2017-07-20 01:30:00 UTC
Description	The Authentication, Authorization, and Accounting (AAA) capability in versions 5.0(1) and 5.0(3) of the software used by mu

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Anomaly Guard Module	5.0(1)	All	All	All
Hardware	Cisco	Anomaly Guard Module	5.0(3)	All	All	All
Hardware	Cisco	Anomaly Guard Module	5.0\(1\)	All	All	All
Hardware	Cisco	Anomaly Guard Module	5.0\(3\)	All	All	All
Hardware	Cisco	Anomaly Guard Module	5.0\(1\)	All	All	All
Hardware	Cisco	Anomaly Guard Module	5.0\(3\)	All	All	All
Hardware	Cisco	Guard	5.0(1)	All	All	All
Hardware	Cisco	Guard	5.0(3)	All	All	All
Hardware	Cisco	Guard	5.0\(1\)	All	All	All
Hardware	Cisco	Guard	5.0\(3\)	All	All	All
Hardware	Cisco	Guard	5.0\(1\)	All	All	All
Hardware	Cisco	Guard	5.0\(3\)	All	All	All
Hardware	Cisco	Traffic Anomaly Detector Module	5.0(1)	All	All	All
Hardware	Cisco	Traffic Anomaly Detector Module	5.0(3)	All	All	All
Hardware	Cisco	Traffic Anomaly Detector Module	5.0\(1\)	All	All	All
Hardware	Cisco	Traffic Anomaly Detector Module	5.0\(3\)	All	All	All
Hardware	Cisco	Traffic Anomaly Detector Module	5.0\(1\)	All	All	All

Hardware	Cisco	Traffic Anomaly Detector Module	5.0\(3\)	All	All	All

References

Reference	Source
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
SecurityTracker.com Archives - Cisco Traffic Anomaly Detector May Let Remote Users Bypass TACACS+ Authentication	SECTRACK
IBM X-Force Exchange	XF
Cisco Multiple Products TACACS+ Authentication Bypass Vulnerability	BID
SecurityTracker.com Archives - Cisco Guard May Let Remote Users Bypass TACACS+ Authentication	SECTRACK
SecurityReason	SREASON
TACACS+ Authentication Bypass in Cisco Anomaly Detection and Mitigation Products [Products & Services] - Cisco Systems	CISCO
23237	OSVDB
Cisco Products TACACS+ Authentication Bypass - Advisories - Secunia	SECUNIA
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.