



# CVE-2006-0764

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

## Summary

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

## 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.

© [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](#)