



CVE-2006-4909

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2006-4909
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-09-21 00:07:00 UTC
Updated	2017-07-20 01:33:00 UTC
Description	Cross-site scripting (XSS) vulnerability in Cisco Guard DDoS Mitigation Appliance before 5.1(6), when anti-spoofing is enab

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Guard Ddos Mitigation Appliance	All	All	All	All
Hardware	Cisco	Guard Ddos Mitigation Appliance	All	All	All	All

References

Reference	Source
Cisco Guard "meta-refresh" Cross-Site Scripting Vulnerability - Advisories - Secunia	SECUNIA
Cisco - Networking, Cloud, and Cybersecurity Solutions	CISCO
SecurityTracker.com Archives - Cisco Guard Input Validation Flaw in Anti-Spoofing Feature Permits Cross-Site Scripting Attacks	SECTRAC
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
IBM X-Force Exchange	XF
Cisco Guard Meta-Refresh Cross-Site Scripting Vulnerability	BID
29035	OSVDB
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](#)