



CVE-2006-4650

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2006-4650
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-09-09 00:04:00 UTC
Updated	2018-10-17 21:38:00 UTC
Description	Cisco IOS 12.0, 12.1, and 12.2, when GRE IP tunneling is used and the RFC2784 compliance fixes are missing, does not v

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	12.0	All	All	All
Operating System	Cisco	ios	12.1	All	All	All
Operating System	Cisco	ios	12.2	All	All	All
Operating System	Cisco	ios	12.0	All	All	All
Operating System	Cisco	ios	12.1	All	All	All
Operating System	Cisco	ios	12.2	All	All	All

References

Reference	Source	Link
SecurityTracker.com Archives - Cisco IOS GRE Parsing Error May Let Remote Users Inject Packets	SECTrack	securitytracker.com
28590	OSVDB	www.osvdb.org
Cisco IOS GRE Decapsulation Vulnerability - Advisories - Secunia	SECUNIA	secunia.com
Repository / Oval Repository	OVAl	oval.cisecurity.org
IBM X-Force Exchange	XF	exchange.xforce.ib
PHENOELIT	MISC	www.phenoelit.de
SecurityFocus	BUGTRAQ	www.securityfocus
SecurityReason - Cisco IOS GRE issue	SREASON	securityreason.com

Cisco Security Response to: Cisco IOS GRE Decapsulation Vulnerability [IP Tunneling] - Cisco Systems	CISCO	www.cisco.com
Webmail- OVH	VUPEN	www.vupen.com
Cisco IOS Multiple GRE Source Routing Vulnerabilities	BID	www.securityfocus
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

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