



CVE-2013-3436

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

Summary

CVE	CVE-2013-3436
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-07-19 14:36:00 UTC
Updated	2017-11-29 02:29:00 UTC
Description	The default configuration of the Group Encrypted Transport VPN (GET VPN) feature on Cisco IOS uses an improper mech

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	ios	-	All	All	All
Operating System	Cisco	ios	-	All	All	All

References

Reference	Source	Link
Cisco Security Notice: Cisco IOS GET VPN Encryption Policy Bypass Vulnerability	CISCO	tools.cisco.c
Cisco IOS Group Encrypted Transport VPN Bug Lets Remote Users Bypass Encryption Policy - SecurityTracker	SECTrack	www.securit
IBM X-Force Exchange	XF	exchange.xl
Cisco IOS GET VPN Encryption Policy CVE-2013-3436 Security Bypass Vulnerability	BID	www.securit
Cisco IOS GET VPN Encryption Policy Bypass Vulnerability	CONFIRM	tools.cisco.c
95460	OSVDB	osvdb.org
CVE Program record	CVE.ORG	www.cve.or
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](#) 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)