



CVE-2011-2678

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

Summary

CVE	CVE-2011-2678
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-07-07 19:55:00 UTC
Updated	2018-10-09 19:32:00 UTC
Description	The Cisco VPN Client 5.0.7.0240 and 5.0.7.0290 on 64-bit Windows platforms uses weak permissions (NT AUTHORITY\IN

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Vpn Client	5.0.7.0240	All	All	All
Application	Cisco	Vpn Client	5.0.7.0290	All	All	All
Application	Cisco	Vpn Client	5.0.7.0240	All	All	All
Application	Cisco	Vpn Client	5.0.7.0290	All	All	All
Operating System	Microsoft	Windows	All	All	All	All
Operating System	Microsoft	Windows	All	All	All	All

References

Reference	Source	Link
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
ISC Diary Deja-Vu: Cisco VPN Windows Client Privilege Escalation	MISC	isc.sans.edu
SecurityFocus	BUGTRAQ	www.securityfocus.com
CCO Redirect	CISCO	www.cisco.com
NGS00051 Technical Advisory: Cisco VPN Client Privilege Escalation - SecurityReason.com	SREASON	securityreason.com
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](#) 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](#)