



CVE-2007-5562

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

Summary

CVE	CVE-2007-5562
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-10-18 20:17:00 UTC
Updated	2017-07-29 01:33:00 UTC
Description	Cross-site scripting (XSS) vulnerability in cgi-bin/welcome (aka the login page) in Netgear SSL312 PROSAFE SSL VPN-Cc

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	Ssl312	All	All	All	All
Hardware	Netgear	Ssl312	All	All	All	All

References

Reference	Source
IBM X-Force Exchange	XF
www.smash-the-stack.net/articles/Netgear_SSL312_XSS_Advisory.txt	MISC
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUP
NETGEAR SSL312 PROSAFE SSL VPN-Concentrator 25 Error Page Cross Site Scripting Vulnerability	BID
Netgear SSL312 "err" Cross-Site Scripting Vulnerability - Advisories - Secunia	SEC
SecurityTracker.com Archives - NETGEAR ProSafe SSL VPN Concentrator Input Validation Hole Permits Cross-Site Scripting Attacks	SEC
20071013 Netgear SSL312 XSS vulnerability	FULL
CVE Program record	CVE
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](#).

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

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