



CVE-2014-7285

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

Summary

CVE	CVE-2014-7285
State	PUBLIC
Assigner	secure@symantec.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-12-17 16:59:00 UTC
Updated	2017-01-03 02:59:00 UTC
Description	The management console on the Symantec Web Gateway (SWG) appliance before 5.2.2 allows remote authenticated user

Risk And Classification

Problem Types: CWE-77

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Symantec	Web Gateway	All	All	All	All

References

Reference
Security Advisories Relating to Symantec Products - Symantec Web Gateway OS Authenticated Command Injection - 2014-12-16T10:15:17 F
Symantec Web Gateway Lets Remote Authenticated Users Execute Arbitrary Commands - SecurityTracker
Symantec Web Gateway <= 5.2.1 (restore.php) OS Command Injection Vulnerability Karma(In)Security
116009
Symantec Web Gateway 5 restore.php Command Injection ≈ Packet Storm
Symantec Web Gateway CVE-2014-7285 Command Injection Vulnerability
Symantec Web Gateway 5 restore.php Post Authentication Command Injection
CVE Program record
NVD vulnerability detail

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](#)