



CVE-2016-5313

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

Summary

CVE	CVE-2016-5313
State	PUBLIC
Assigner	secure@symantec.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-12 22:59:00 UTC
Updated	2017-04-20 13:31:00 UTC
Description	Symantec Web Gateway (SWG) before 5.2.5 allows remote authenticated users to execute arbitrary OS commands.

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference
Symantec Web Gateway CVE-2016-5313 Command Injection Vulnerability
Full Disclosure: [KIS-2016-12] Magento <= 1.9.2.2 (RSS Feed) Information Disclosure Vulnerability
Symantec Web Gateway 5.2.2 OS Command Injection ~ Packet Storm
Security Advisories Relating to Symantec Products - Symantec Web Gateway Management Console Interface Command Injection - 2016-10-01
Symantec Web Gateway Bug Lets Remote Authenticated Users Modify the Whitelist Configuration - SecurityTracker
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.

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