



CVE-2017-18001

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2017-18001
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-31 19:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	Trustwave Secure Web Gateway (SWG) through 11.8.0.27 allows remote attackers to append an arbitrary public key to the

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Trustwave	Secure Web Gateway	All	All	All	All

References

Reference	Source	Link	Tags
SWG vulnerability version 11.8 and earlier Trustwave	MISC	www.trustwave.com	Vendor Advisory
SSD Advisory – Trustwave SWG Unauthorized Access - SSD Secure Disclosure	MISC	blogs.securiteam.com	Exploit, Third Party
Full Disclosure: SSD Advisory – Trustwave SWG Unauthorized Access	MISC	seclists.org	Exploit, Mailing List
Trustwave SWG 11.8.0.27 - SSH Unauthorized Access	EXPLOIT-DB	www.exploit-db.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

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