



CVE-2015-8675

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

Summary

CVE	CVE-2015-8675
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-01-15 19:59:00 UTC
Updated	2016-01-21 17:29:00 UTC
Description	Huawei S5300 Campus Series switches with software before V200R005SPH008 do not mask the password when uploadin

Risk And Classification

Problem Types: CWE-255

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Huawei	S5300	All	All	All	All
Hardware	Huawei	S5300	All	All	All	All
Operating System	Huawei	S5300 Firmware	v200r005c02	All	All	All
Operating System	Huawei	S5300 Firmware	v200r005c02	All	All	All

References

Reference	Source	Link	Tags
Security Advisory - Information Exposure Vulnerability in Huawei Ethernet Switch	CONFIRM	www.huawei.com	Vendor Advisory
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.

Legacy QID Mappings

[43853](#) Huawei Switch Information Exposure Vulnerability (Huawei-SA-20160112-01-Switch)

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](#).

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