



CVE-2018-5967

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

Summary

CVE	CVE-2018-5967
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-25 08:29:00 UTC
Updated	2018-02-12 14:31:00 UTC
Description	Netis WF2419 V2.2.36123 devices allow XSS via the Description parameter on the Bandwidth Control Rule Settings page.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netis-systems	Wf2419	-	All	All	All
Hardware	Netis-systems	Wf2419	-	All	All	All
Operating System	Netis-systems	Wf2419 Firmware	2.2.36123	All	All	All
Operating System	Netis-systems	Wf2419 Firmware	2.2.36123	All	All	All

References

Reference	Source	Link	Tags
Netis-WF2419 HTML Injection ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit, Third Party Advisory, VDB Entry
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.

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