



CVE-2014-4871

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2014-4871
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-07 10:55:00 UTC
Updated	2015-10-06 02:38:00 UTC
Description	Cross-site scripting (XSS) vulnerability in wsecurity.html on NetCommWireless NB604N routers with firmware before GAN5

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netcommwireless	Nb604n	-	All	All	All
Hardware	Netcommwireless	Nb604n	-	All	All	All
Operating System	Netcommwireless	Nb604n Firmware	All	All	All	All

References

Reference

- Vulnerability Note VU#941108 - NetCommWireless NB604N ADSL2+ Wireless N300 Modem Router contains a stored cross-site scripting vuln
- NetCommWireless NB604N ADSL2+ Router 'wsecurity.html' HTML Injection Vulnerability
- 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.

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](#)