



CVE-2018-6000

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

Summary

CVE	CVE-2018-6000
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-22 20:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	An issue was discovered in AsusWRT before 3.0.0.4.384_10007. The do_vpnupload_post function in router/httpd/web.c in

Risk And Classification

Problem Types: CWE-862

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Asus	Asuswrt	All	All	All	All
Operating System	Asus	Asuswrt	All	All	All	All

References

Reference	Source	Link
AsusWRT LAN - Remote Code Execution (Metasploit) - Hardware remote Exploit	EXPLOIT-DB	www.exploit-db.com
AsusWRT Router < 3.0.0.4.380.7743 - LAN Remote Code Execution - Hardware remote Exploit	EXPLOIT-DB	www.exploit-db.com
PoC/asuswrt-lan-rce.txt at master · pedrib/PoC · GitHub	MISC	github.com
401 Authorization Required	MISC	blogs.securiteam.com
raw.githubusercontent.com/pedrib/PoC/master/exploits/metasploit/asuswrt_lan_rce.rb	MISC	raw.githubusercontent.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

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](#)