



CVE-2018-11106

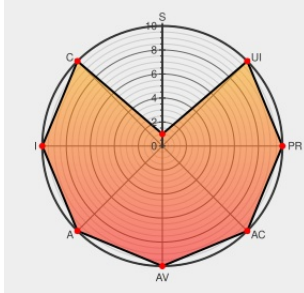
Published on: 04/01/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:18 PM UTC

CVE-2018-11106

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of **Wc7500** from **Netgear** contain the following vulnerability:

NETGEAR has released fixes for a pre-authentication command injection in request_handler.php security vulnerability on the following product models: WC7500, running firmware versions prior to 6.5.3.5; WC7520, running firmware versions prior to 2.5.0.46; WC7600v1, running firmware versions prior to 6.5.3.5; WC7600v2, running firmware versions prior to 6.5.3.5; and WC9500, running firmware versions prior to 6.5.3.5.

CVE-2018-11106 has been assigned by **N** security@netgear.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **N** **NETGEAR - WC7500** version **firmware versions prior to 6.5.3.5**

Affected Vendor/Software: **N** **NETGEAR - WC7520** version **firmware versions prior to 2.5.0.46**

Affected Vendor/Software: **N** **NETGEAR - WC7600v1** version **firmware versions prior to 6.5.3.5**

Affected Vendor/Software: **N** **NETGEAR - WC7600v2** version **firmware versions prior to 6.5.3.5**

Affected Vendor/Software: **N** **NETGEAR - WC9500** version **firmware versions prior to 6.5.3.5**

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **10 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE

Confidentiality Impact	Integrity Impact	Availability Impact				
COMPLETE	COMPLETE	COMPLETE				
CVE References						
Description	Tags	Link				
Security Advisory for Pre-Authentication Command Injection in request_handler.php on Some Wireless Controllers, PSV-2018-0051 Answer NETGEAR Support	Patch Vendor Advisory kb.netgear.com text/html	N CONFIRM kb.netgear.com/000058243/Security-Advisory-for-Pre-Authentication-Command-Injection-in-request-handler-php-on-Some-Wireless-Controllers-PSV-2018-0051				
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.						
There are currently no QIDs associated with this CVE						
Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Hardware  	Netgear	Wc7500	-	All	All	All
Hardware  	Netgear	Wc7500	-	All	All	All
Operating System	Netgear	Wc7500 Firmware	All	All	All	All
Operating System	Netgear	Wc7500 Firmware	All	All	All	All
Hardware  	Netgear	Wc7520	-	All	All	All
Hardware  	Netgear	Wc7520	-	All	All	All
Operating System	Netgear	Wc7520 Firmware	All	All	All	All
Operating System	Netgear	Wc7520 Firmware	All	All	All	All
Hardware  	Netgear	Wc7600v1	-	All	All	All
Hardware  	Netgear	Wc7600v1	-	All	All	All
Operating System	Netgear	Wc7600v1 Firmware	All	All	All	All
Operating System	Netgear	Wc7600v1 Firmware	All	All	All	All
Hardware  	Netgear	Wc7600v2	-	All	All	All
Hardware  	Netgear	Wc7600v2	-	All	All	All
Operating System	Netgear	Wc7600v2 Firmware	All	All	All	All

Operating System	Netgear	Wc7600v2 Firmware	All	All	All	All
Hardware 🚩🔗	Netgear	Wc9500	-	All	All	All
Hardware 🚩🔗	Netgear	Wc9500	-	All	All	All
Operating System	Netgear	Wc9500 Firmware	All	All	All	All
Operating System	Netgear	Wc9500 Firmware	All	All	All	All
cpe:2.3:h:netgear:wc7500:-:*:*:*:*:*:						
cpe:2.3:h:netgear:wc7500:-:*:*:*:*:*:						
cpe:2.3:o:netgear:wc7500_firmware:*:*:*:*:*:						
cpe:2.3:o:netgear:wc7500_firmware:*:*:*:*:*:						
cpe:2.3:h:netgear:wc7520:-:*:*:*:*:*:						
cpe:2.3:h:netgear:wc7520:-:*:*:*:*:*:						
cpe:2.3:o:netgear:wc7520_firmware:*:*:*:*:*:						
cpe:2.3:o:netgear:wc7520_firmware:*:*:*:*:*:						
cpe:2.3:h:netgear:wc7600v1:-:*:*:*:*:*:						
cpe:2.3:h:netgear:wc7600v1:-:*:*:*:*:*:						
cpe:2.3:o:netgear:wc7600v1_firmware:*:*:*:*:*:						
cpe:2.3:o:netgear:wc7600v1_firmware:*:*:*:*:*:						
cpe:2.3:h:netgear:wc7600v2:-:*:*:*:*:*:						
cpe:2.3:h:netgear:wc7600v2:-:*:*:*:*:*:						
cpe:2.3:o:netgear:wc7600v2_firmware:*:*:*:*:*:						
cpe:2.3:o:netgear:wc7600v2_firmware:*:*:*:*:*:						
cpe:2.3:h:netgear:wc9500:-:*:*:*:*:*:						
cpe:2.3:h:netgear:wc9500:-:*:*:*:*:*:						
cpe:2.3:o:netgear:wc9500_firmware:*:*:*:*:*:						
cpe:2.3:o:netgear:wc9500_firmware:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© [CVE.report](#) 2023   |

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](#)