



# CVE-2018-21097

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

## Summary

<b>CVE</b>	CVE-2018-21097
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-04-27 16:15:00 UTC
<b>Updated</b>	2020-05-04 14:15:00 UTC
<b>Description</b>	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects WAC

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	Wac120	-	All	All	All
Hardware	Netgear	Wac120	-	All	All	All
Operating System	Netgear	Wac120 Firmware	All	All	All	All
Operating System	Netgear	Wac120 Firmware	All	All	All	All
Hardware	Netgear	Wac505	-	All	All	All
Hardware	Netgear	Wac505	-	All	All	All
Operating System	Netgear	Wac505 Firmware	All	All	All	All
Operating System	Netgear	Wac505 Firmware	All	All	All	All
Hardware	Netgear	Wac510	-	All	All	All
Hardware	Netgear	Wac510	-	All	All	All
Operating System	Netgear	Wac510 Firmware	All	All	All	All
Operating System	Netgear	Wac510 Firmware	All	All	All	All
Hardware	Netgear	Wn604	-	All	All	All
Hardware	Netgear	Wn604	-	All	All	All
Operating System	Netgear	Wn604 Firmware	All	All	All	All
Operating System	Netgear	Wn604 Firmware	All	All	All	All
Hardware	Netgear	Wnap210	v2	All	All	All

Hardware	<a href="#">Netgear</a>	<a href="#">Wnap210</a>	v2	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wnap210 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wnap210 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wnap320</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wnap320</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wnap320 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wnap320 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wnd930</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wnd930</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wnd930 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wnd930 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wndap350</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wndap350</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wndap350 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wndap350 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wndap360</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wndap360</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wndap360 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wndap360 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wndap620</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wndap620</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wndap620 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wndap620 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wndap660</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wndap660</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wndap660 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wndap660 Firmware</a>	All	All	All	All

## References

### Reference

[Security Advisory for Pre-Authentication Stack Overflow on Some Wireless Access Points, PSV-2018-0094 | Answer | NETGEAR Support](#)

[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.

© [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](#)