



CVE-2018-21215

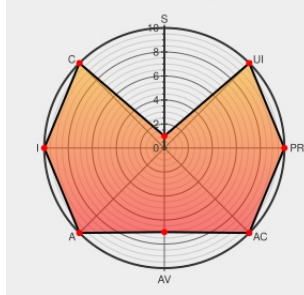
Published on: 04/28/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:35 PM UTC

CVE-2018-21215

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

CVSS:30/AC:L/AV:A/H/C:H/I:H/PR:N/S:U/UI:N



Certain versions of **D3600** from **Netgear** contain the following vulnerability:

Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, EX2700 before 1.0.1.28, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, and WN3100RPv2 before 1.0.0.56.

CVE-2018-21215 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **5.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Security Advisory for Pre-Authentication Buffer Overflow on Some Routers, Gateways, and Extenders, PSV-2017-2486	Vendor Advisory kb.netgear.com	N CONFIRM kb.netgear.com/000055122/Security-Advisory-for-Pre-Authentication-Buffer-Overflow-on-

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	D3600	-	All	All	All
Hardware 	Netgear	D3600	-	All	All	All
Operating System	Netgear	D3600 Firmware	All	All	All	All
Operating System	Netgear	D3600 Firmware	All	All	All	All
Hardware 	Netgear	D6000	-	All	All	All
Hardware 	Netgear	D6000	-	All	All	All
Operating System	Netgear	D6000 Firmware	All	All	All	All
Operating System	Netgear	D6000 Firmware	All	All	All	All
Hardware 	Netgear	D6100	-	All	All	All
Hardware 	Netgear	D6100	-	All	All	All
Operating System	Netgear	D6100 Firmware	All	All	All	All
Operating System	Netgear	D6100 Firmware	All	All	All	All
Hardware 	Netgear	Ex2700	-	All	All	All
Hardware 	Netgear	Ex2700	-	All	All	All
Operating System	Netgear	Ex2700 Firmware	All	All	All	All
Operating System	Netgear	Ex2700 Firmware	All	All	All	All
Hardware 	Netgear	R7500	v2	All	All	All
Hardware 	Netgear	R7500	v2	All	All	All
Operating System	Netgear	R7500 Firmware	All	All	All	All
Operating System	Netgear	R7500 Firmware	All	All	All	All

System						
Hardware 	Netgear	R9000	-	All	All	All
Hardware 	Netgear	R9000	-	All	All	All
Operating System	Netgear	R9000 Firmware	All	All	All	All
Operating System	Netgear	R9000 Firmware	All	All	All	All
Hardware 	Netgear	Wn2000rpt	v3	All	All	All
Hardware 	Netgear	Wn2000rpt	v3	All	All	All
Operating System	Netgear	Wn2000rpt Firmware	All	All	All	All
Operating System	Netgear	Wn2000rpt Firmware	All	All	All	All
Hardware 	Netgear	Wn3000rp	v3	All	All	All
Hardware 	Netgear	Wn3000rp	v3	All	All	All
Operating System	Netgear	Wn3000rp Firmware	All	All	All	All
Operating System	Netgear	Wn3000rp Firmware	All	All	All	All
Hardware 	Netgear	Wn3100rp	v2	All	All	All
Hardware 	Netgear	Wn3100rp	v2	All	All	All
Operating System	Netgear	Wn3100rp Firmware	All	All	All	All
Operating System	Netgear	Wn3100rp Firmware	All	All	All	All
cpe:2.3:h:netgear:d3600:-:*~::~:						
cpe:2.3:h:netgear:d3600:-:*~::~:						
cpe:2.3:o:netgear:d3600_firmware:*~::~:						
cpe:2.3:o:netgear:d3600_firmware:*~::~:						
cpe:2.3:h:netgear:d6000:-:*~::~:						
cpe:2.3:h:netgear:d6000:-:*~::~:						
cpe:2.3:o:netgear:d6000_firmware:*~::~:						
cpe:2.3:o:netgear:d6000_firmware:*~::~:						
cpe:2.3:h:netgear:d6100:-:*~::~:						
cpe:2.3:h:netgear:d6100:-:*~::~:						
cpe:2.3:o:netgear:d6100_firmware:*~::~:						

cpe:2.3:o:netgear:d6100_firmware:*.*.*.*.*.*.*.*.*.*
cpe:2.3:h:netgear:ex2700:-.*.*.*.*.*.*.*.*.*.*
cpe:2.3:h:netgear:ex2700:-.*.*.*.*.*.*.*.*.*.*
cpe:2.3:o:netgear:ex2700_firmware:*.*.*.*.*.*.*.*.*.*
cpe:2.3:o:netgear:ex2700_firmware:*.*.*.*.*.*.*.*.*.*
cpe:2.3:h:netgear:r7500:v2:*.*.*.*.*.*.*.*.*.*
cpe:2.3:h:netgear:r7500:v2:*.*.*.*.*.*.*.*.*.*
cpe:2.3:o:netgear:r7500_firmware:*.*.*.*.*.*.*.*.*.*
cpe:2.3:o:netgear:r7500_firmware:*.*.*.*.*.*.*.*.*.*
cpe:2.3:h:netgear:r9000:-.*.*.*.*.*.*.*.*.*.*
cpe:2.3:h:netgear:r9000:-.*.*.*.*.*.*.*.*.*.*
cpe:2.3:o:netgear:r9000_firmware:*.*.*.*.*.*.*.*.*.*
cpe:2.3:o:netgear:r9000_firmware:*.*.*.*.*.*.*.*.*.*
cpe:2.3:h:netgear:wn2000rpt:v3:*.*.*.*.*.*.*.*.*.*
cpe:2.3:h:netgear:wn2000rpt:v3:*.*.*.*.*.*.*.*.*.*
cpe:2.3:o:netgear:wn2000rpt_firmware:*.*.*.*.*.*.*.*.*.*
cpe:2.3:o:netgear:wn2000rpt_firmware:*.*.*.*.*.*.*.*.*.*
cpe:2.3:h:netgear:wn3000rp:v3:*.*.*.*.*.*.*.*.*.*
cpe:2.3:h:netgear:wn3000rp:v3:*.*.*.*.*.*.*.*.*.*
cpe:2.3:o:netgear:wn3000rp_firmware:*.*.*.*.*.*.*.*.*.*
cpe:2.3:o:netgear:wn3000rp_firmware:*.*.*.*.*.*.*.*.*.*
cpe:2.3:h:netgear:wn3100rp:v2:*.*.*.*.*.*.*.*.*.*
cpe:2.3:h:netgear:wn3100rp:v2:*.*.*.*.*.*.*.*.*.*
cpe:2.3:o:netgear:wn3100rp_firmware:*.*.*.*.*.*.*.*.*.*
cpe:2.3:o:netgear:wn3100rp_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](#)