



# CVE-2018-21223

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

## Summary

<b>CVE</b>	CVE-2018-21223
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-04-28 17:15:00 UTC
<b>Updated</b>	2020-05-05 19:19:00 UTC
<b>Description</b>	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.

## Risk And Classification

**Problem Types:** CWE-120

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Netgear</a>	D3600	-	All	All	All
Hardware	<a href="#">Netgear</a>	D3600	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">D3600 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">D3600 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	D6000	-	All	All	All
Hardware	<a href="#">Netgear</a>	D6000	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">D6000 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">D6000 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	D7800	-	All	All	All
Hardware	<a href="#">Netgear</a>	D7800	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">D7800 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">D7800 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	R6100	-	All	All	All
Hardware	<a href="#">Netgear</a>	R6100	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R6100 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R6100 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	R7500	-	All	All	All

Hardware	<a href="#">Netgear</a>	<a href="#">R7500</a>	v2	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">R7500</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">R7500</a>	v2	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R7500 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R7500 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">R9000</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">R9000</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R9000 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">R9000 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wndr3700</a>	v4	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wndr3700</a>	v4	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wndr3700 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wndr3700 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wndr4300</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wndr4300</a>	v2	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wndr4300</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wndr4300</a>	v2	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wndr4300 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wndr4300 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wndr4500</a>	v3	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wndr4500</a>	v3	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wndr4500 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wndr4500 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wnr2000</a>	v5	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wnr2000</a>	v5	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wnr2000 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wnr2000 Firmware</a>	All	All	All	All

## References

### Reference

[Security Advisory for Pre-Authentication Buffer Overflow on Some Routers and Gateways, PSV-2017-2457 | 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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)