



CVE-2018-21145

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2018-21145 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-04-21 22:15:00 UTC |
| Updated | 2020-04-27 15:44:00 UTC |
| Description | Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 bef |

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------------------|--------------------------------|---------|--------|---------|----------|
| Hardware | Netgear | D7800 | - | All | All | All |
| Hardware | Netgear | D7800 | - | All | All | All |
| Operating System | Netgear | D7800 Firmware | All | All | All | All |
| Operating System | Netgear | D7800 Firmware | All | All | All | All |
| Hardware | Netgear | Dm200 | - | All | All | All |
| Hardware | Netgear | Dm200 | - | All | All | All |
| Operating System | Netgear | Dm200 Firmware | All | All | All | All |
| Operating System | Netgear | Dm200 Firmware | All | All | All | All |
| Hardware | Netgear | R6100 | - | All | All | All |
| Hardware | Netgear | R6100 | - | All | All | All |
| Operating System | Netgear | R6100 Firmware | All | All | All | All |
| Operating System | Netgear | R6100 Firmware | All | All | All | All |
| Hardware | Netgear | R7500 | - | All | All | All |
| Hardware | Netgear | R7500 | - | All | All | All |
| Operating System | Netgear | R7500 Firmware | All | All | All | All |
| Operating System | Netgear | R7500 Firmware | All | All | All | All |
| Hardware | Netgear | R7800 | - | All | All | All |

| | | | | | | |
|------------------|-------------------------|-----------------------------------|-----|-----|-----|-----|
| Hardware | Netgear | R7800 | - | All | All | All |
| Operating System | Netgear | R7800 Firmware | All | All | All | All |
| Operating System | Netgear | R7800 Firmware | All | All | All | All |
| Hardware | Netgear | R8900 | - | All | All | All |
| Hardware | Netgear | R8900 | - | All | All | All |
| Operating System | Netgear | R8900 Firmware | All | All | All | All |
| Operating System | Netgear | R8900 Firmware | All | All | All | All |
| 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 | Wnvr3700 | v4 | All | All | All |
| Hardware | Netgear | Wnvr3700 | v4 | All | All | All |
| Operating System | Netgear | Wnvr3700 Firmware | All | All | All | All |
| Operating System | Netgear | Wnvr3700 Firmware | All | All | All | All |
| Hardware | Netgear | Wnvr4300 | - | All | All | All |
| Hardware | Netgear | Wnvr4300 | v2 | All | All | All |
| Hardware | Netgear | Wnvr4300 | - | All | All | All |
| Hardware | Netgear | Wnvr4300 | v2 | All | All | All |
| Operating System | Netgear | Wnvr4300 Firmware | All | All | All | All |
| Operating System | Netgear | Wnvr4300 Firmware | All | All | All | All |
| Hardware | Netgear | Wnvr4500 | v3 | All | All | All |
| Hardware | Netgear | Wnvr4500 | v3 | All | All | All |
| Operating System | Netgear | Wnvr4500 Firmware | All | All | All | All |
| Operating System | Netgear | Wnvr4500 Firmware | All | All | All | All |
| Hardware | Netgear | Wnr2000 | v5 | All | All | All |
| Hardware | Netgear | Wnr2000 | v5 | All | All | All |
| Operating System | Netgear | Wnr2000 Firmware | All | All | All | All |
| Operating System | Netgear | Wnr2000 Firmware | All | All | All | All |

References

Reference

Security Advisory for Post-Authentication Stack Overflow on Some Gateways and Routers, PSV-2017-3160 | 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](#)