



CVE-2020-35840

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2020-35840 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-12-30 00:15:00 UTC |
| Updated | 2020-12-31 20:13:00 UTC |
| Description | Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.38, D7000 before 1.0.1.78, JNR1 |

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------------------|--------------------|---------|--------|---------|----------|
| Hardware | Netgear | D6200 | - | All | All | All |
| Hardware | Netgear | D6200 | - | All | All | All |
| Operating System | Netgear | D6200 Firmware | All | All | All | All |
| Operating System | Netgear | D6200 Firmware | All | All | All | All |
| Hardware | Netgear | D7000 | - | All | All | All |
| Hardware | Netgear | D7000 | - | All | All | All |
| Operating System | Netgear | D7000 Firmware | All | All | All | All |
| Operating System | Netgear | D7000 Firmware | All | All | All | All |
| Hardware | Netgear | Jnr1010v2 | - | All | All | All |
| Hardware | Netgear | Jnr1010v2 | - | All | All | All |
| Operating System | Netgear | Jnr1010v2 Firmware | All | All | All | All |
| Operating System | Netgear | Jnr1010v2 Firmware | All | All | All | All |
| Hardware | Netgear | Jr6150 | - | All | All | All |
| Hardware | Netgear | Jr6150 | - | All | All | All |
| Operating System | Netgear | Jr6150 Firmware | All | All | All | All |
| Operating System | Netgear | Jr6150 Firmware | All | All | All | All |
| Hardware | Netgear | Jwnr2010v5 | - | All | All | All |

| | | | | | | |
|------------------|---------|---------------------|-----|-----|-----|-----|
| Hardware | Netgear | Jwnr2010v5 | - | All | All | All |
| Operating System | Netgear | Jwnr2010v5 Firmware | All | All | All | All |
| Operating System | Netgear | Jwnr2010v5 Firmware | All | All | All | All |
| Hardware | Netgear | R6020 | - | All | All | All |
| Hardware | Netgear | R6020 | - | All | All | All |
| Operating System | Netgear | R6020 Firmware | All | All | All | All |
| Operating System | Netgear | R6020 Firmware | All | All | All | All |
| Hardware | Netgear | R6050 | - | All | All | All |
| Hardware | Netgear | R6050 | - | All | All | All |
| Operating System | Netgear | R6050 Firmware | All | All | All | All |
| Operating System | Netgear | R6050 Firmware | All | All | All | All |
| Hardware | Netgear | R6080 | - | All | All | All |
| Hardware | Netgear | R6080 | - | All | All | All |
| Operating System | Netgear | R6080 Firmware | All | All | All | All |
| Operating System | Netgear | R6080 Firmware | All | All | All | All |
| Hardware | Netgear | R6120 | - | All | All | All |
| Hardware | Netgear | R6120 | - | All | All | All |
| Operating System | Netgear | R6120 Firmware | All | All | All | All |
| Operating System | Netgear | R6120 Firmware | All | All | All | All |
| Hardware | Netgear | R6220 | - | All | All | All |
| Hardware | Netgear | R6220 | - | All | All | All |
| Operating System | Netgear | R6220 Firmware | All | All | All | All |
| Operating System | Netgear | R6220 Firmware | All | All | All | All |
| Hardware | Netgear | R6260 | - | All | All | All |
| Hardware | Netgear | R6260 | - | All | All | All |
| Operating System | Netgear | R6260 Firmware | All | All | All | All |
| Operating System | Netgear | R6260 Firmware | All | All | All | All |
| Hardware | Netgear | Wnr1000v4 | - | All | All | All |
| Hardware | Netgear | Wnr1000v4 | - | All | All | All |
| Operating System | Netgear | Wnr1000v4 Firmware | All | All | All | All |
| Operating System | Netgear | Wnr1000v4 Firmware | All | All | All | All |
| Hardware | Netgear | Wnr2020 | - | All | All | All |
| Hardware | Netgear | Wnr2020 | - | All | All | All |
| Operating System | Netgear | Wnr2020 Firmware | All | All | All | All |
| Operating System | Netgear | Wnr2020 Firmware | All | All | All | All |

| | | | | | | |
|------------------|-------------------------|----------------------------------|-----|-----|-----|-----|
| Hardware | Netgear | Wnr2050 | - | All | All | All |
| Hardware | Netgear | Wnr2050 | - | All | All | All |
| Operating System | Netgear | Wnr2050 Firmware | All | All | All | All |
| Operating System | Netgear | Wnr2050 Firmware | All | All | All | All |

References

| Reference | Source | Link |
|---|---------|--------------------------------|
| Security Advisory for Stored Cross Site Scripting on Some Routers, PSV-2019-0010 Answer NETGEAR Support | MISC | kb.netgear.com |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

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](#)