



# CVE-2019-20752

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

## Summary

<b>CVE</b>	CVE-2019-20752
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-04-16 22:15:00 UTC
<b>Updated</b>	2020-04-23 19:45:00 UTC
<b>Description</b>	Certain NETGEAR devices are affected by stored XSS. This affects D3600 before 1.0.0.75, D6000 before 1.0.0.75, D7800

## Risk And Classification

**Problem Types:** CWE-79

## 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>	Dm200	-	All	All	All
Hardware	<a href="#">Netgear</a>	Dm200	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Dm200 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Dm200 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	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	Rbk20	-	All	All	All
Hardware	Netgear	Rbk20	-	All	All	All
Operating System	Netgear	Rbk20 Firmware	All	All	All	All
Operating System	Netgear	Rbk20 Firmware	All	All	All	All
Hardware	Netgear	Rbk40	-	All	All	All
Hardware	Netgear	Rbk40	-	All	All	All
Operating System	Netgear	Rbk40 Firmware	All	All	All	All
Operating System	Netgear	Rbk40 Firmware	All	All	All	All
Hardware	Netgear	Rbk50	-	All	All	All
Hardware	Netgear	Rbk50	-	All	All	All
Operating System	Netgear	Rbk50 Firmware	All	All	All	All
Operating System	Netgear	Rbk50 Firmware	All	All	All	All
Hardware	Netgear	Rbr20	-	All	All	All
Hardware	Netgear	Rbr20	-	All	All	All
Operating System	Netgear	Rbr20 Firmware	All	All	All	All
Operating System	Netgear	Rbr20 Firmware	All	All	All	All
Hardware	Netgear	Rbr50	-	All	All	All
Hardware	Netgear	Rbr50	-	All	All	All
Operating System	Netgear	Rbr50 Firmware	All	All	All	All
Operating System	Netgear	Rbr50 Firmware	All	All	All	All
Hardware	Netgear	Rbs20	-	All	All	All
Hardware	Netgear	Rbs20	-	All	All	All
Operating System	Netgear	Rbs20 Firmware	All	All	All	All
Operating System	Netgear	Rbs20 Firmware	All	All	All	All

Hardware	<a href="#">Netgear</a>	<a href="#">Rbs40</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbs40</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbs40 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbs40 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbs50</a>	-	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Rbs50</a>	-	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbs50 Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Rbs50 Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wn3000rp</a>	v2	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wn3000rp</a>	v3	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wn3000rp</a>	v2	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wn3000rp</a>	v3	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wn3000rp Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wn3000rp Firmware</a>	All	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wn3100rp</a>	v2	All	All	All
Hardware	<a href="#">Netgear</a>	<a href="#">Wn3100rp</a>	v2	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wn3100rp Firmware</a>	All	All	All	All
Operating System	<a href="#">Netgear</a>	<a href="#">Wn3100rp Firmware</a>	All	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>	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 Site Stored Cross Scripting on Some Gateways, Routers, and WiFi Systems, PSV-2018-0250 | Answer | NETGEAR Sup

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](#)