

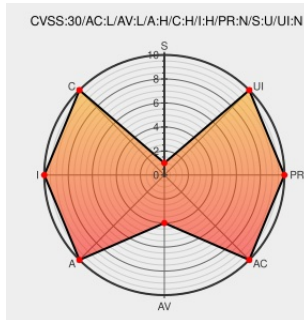


CVE-2017-18779

Published on: 04/22/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:55 PM UTC

CVE-2017-18779

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

Certain versions of **D6200** from **Netgear** contain the following vulnerability:

Certain NETGEAR devices are affected by a buffer overflow. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.12, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.

CVE-2017-18779 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **4.6 - MEDIUM**

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

CVE References

Description	Tags	Link
-------------	------	------

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	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	Jnr1010	v2	All	All	All
Hardware 	Netgear	Jnr1010	v2	All	All	All
Operating System	Netgear	Jnr1010 Firmware	All	All	All	All
Operating System	Netgear	Jnr1010 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	Jwnr2010	v5	All	All	All
Hardware 	Netgear	Jwnr2010	v5	All	All	All
Operating System	Netgear	Jwnr2010 Firmware	All	All	All	All

Operating System	Netgear	Jwnr2010 Firmware	All	All	All	All
Hardware  	Netgear	Pr2000	-	All	All	All
Hardware  	Netgear	Pr2000	-	All	All	All
Operating System	Netgear	Pr2000 Firmware	All	All	All	All
Operating System	Netgear	Pr2000 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	R6700	v2	All	All	All
Hardware  	Netgear	R6700	v2	All	All	All

Hardware  	Netgear	R6700	v2	All	All	All
Operating System	Netgear	R6700 Firmware	All	All	All	All
Operating System	Netgear	R6700 Firmware	All	All	All	All
Hardware  	Netgear	R6800	-	All	All	All
Hardware  	Netgear	R6800	-	All	All	All
Operating System	Netgear	R6800 Firmware	All	All	All	All
Operating System	Netgear	R6800 Firmware	All	All	All	All
Hardware  	Netgear	R6900	v2	All	All	All
Hardware  	Netgear	R6900	v2	All	All	All
Operating System	Netgear	R6900 Firmware	All	All	All	All
Operating System	Netgear	R6900 Firmware	All	All	All	All
Hardware  	Netgear	Wn dr3700	v5	All	All	All
Hardware  	Netgear	Wn dr3700	v5	All	All	All
Operating System	Netgear	Wn dr3700 Firmware	All	All	All	All
Operating System	Netgear	Wn dr3700 Firmware	All	All	All	All
Hardware  	Netgear	Wnr1000	v4	All	All	All
Hardware  	Netgear	Wnr1000	v4	All	All	All
Operating System	Netgear	Wnr1000 Firmware	All	All	All	All
Operating System	Netgear	Wnr1000 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

system

```
cpe:2.3:h:netgear:d6200:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:d6200:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:netgear:d6200_firmware:*:*:*:*:*:*:
```

```
cpe:2.3:o:netgear:d6200_firmware:*.*.*.*.*.*.*.*
```

```
cpe:2.3:h:netgear:d7000:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:d7000:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:netgear:d7000_firmware:*.:*:*:*:*:*:*:
```

```
cpe:2.3:o:netgear:d7000_firmware:*.:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:jnr1010:v2:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:jnr1010:v2:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:netgear:jnr1010_firmware:*.:.:.:.:.:.:
```

```
cpe:2.3:o:netgear:jnr1010_firmware:*:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:jr6150:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:jr6150:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:netgear:jr6150_firmware:*.:*:*:*:*:*:*:
```

```
cpe:2.3:o:netgear:jr6150_firmware:*.:.:.:.:.:.:.:
```

```
cpe:2.3:h:netgear:jwnr2010:v5:*:*:*:*:*:
```

cpe:2.3:h:netgear:jwnr2010:v5:*:*:*:*:*:

```
cpe:2.3:o:netgear:jwnr2010_firmware:*.~*~*~*~*~*~*~*~*~*
```

```
cpe:2.3:o:netgear:jwnr2010_firmware:*.~*~*~*~*~*~*~*~*~*
```

```
cpe:2.3:h:netgear:pr2000:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:pr2000:-:*:*:*:*:*:*:
```

cpe:2.3:o:netgear:pr2000_firmware:*.*.*.*.*.*.*.*

cpe:2.3:o:netgear:pr2000_firmware:*:*:*:*:*:*:

```
cpe:2.3:h:netgear:r6020:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:r6020:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:netgear:r6020_firmware:*.*.*.*.*.*.*.*
```

```
cpe:2.3:o:netgear:r6020_firmware:*.*.*.*.*.*.*.*
```

```
cpe:2.3:h:netgear:r6050:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:r6050:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:netgear:r6050_firmware:*.*.*.*.*.*.*.*
```

```
cpe:2.3:o:netgear:r6050 firmware:*.*.*.*.*.*.*.*
```

```
cpe:2.3:h:netgear:r6080:-:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:r6080:-:*:*:*:*:*:
```

```
cpe:2.3:o:netgear:r6080_firmware:*.*.*.*.*.*.*.*
```

```
cpe:2.3:o:netgear:r6080 firmware:*.~*~*~*~*~*~*
```

```
cpe:2.3:h:netgear:r6120:-:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:r6120:-:*:*:*:*:*:
```

```
cpe:2.3:o:netgear:r6120_firmware:*:*:*:*:*:*:
```

```
cpe:2.3:o:netgear:r6120_firmware:*.*.*.*.*.*.*.*
```

```
cpe:2.3:h:netgear:r6220:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:r6220:-:*:*:*:*:*:
```

```
cpe:2.3:o:netgear:r6220_firmware:*.:*:*:*:*:*:
```

```
cpe:2.3:o:netgear:r6220_firmware:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:r6700:v2:*.~*~*~*~*~*~*
```

```
cpe:2.3:h:netgear:r6700:v2:*:*:*:*:*:
```

```
cpe:2.3:o:netgear:r6700_firmware:*:*:*:*:*.*
```

```
cpe:2.3:o:netgear:r6700 firmware:*.~*~*~*~*~*~*
```

```
cpe:2.3:h:netgear:r6800:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:r6800:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:netgear:r6800_firmware:*:*:*:*:*:*:*:
```

```
cpe:2.3:o:netgear:r6800_firmware:*:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:r6900:v2:*.~*~*~*~*~*~*
```

```
cpe:2.3:h:netgear:r6900:v2:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:netgear:r6900_firmware:*:*:*:*:*:*:*:
```

```
cpe:2.3:o:netgear:r6900_firmware:*:*:*:*:*:*:*:
```

[illegible]

cpe:2.3:h:netgear:wndr3700:v5:*****:
cpe:2.3:h:netgear:wndr3700:v5:*****:
cpe:2.3:o:netgear:wndr3700_firmware:*****:
cpe:2.3:o:netgear:wndr3700_firmware:*****:
cpe:2.3:h:netgear:wnr1000:v4:*****:
cpe:2.3:h:netgear:wnr1000:v4:*****:
cpe:2.3:o:netgear:wnr1000_firmware:*****:
cpe:2.3:o:netgear:wnr1000_firmware:*****:
cpe:2.3:h:netgear:wnr2020:-:*****:
cpe:2.3:h:netgear:wnr2020:-:*****:
cpe:2.3:o:netgear:wnr2020_firmware:*****:
cpe:2.3:o:netgear:wnr2020_firmware:*****:
cpe:2.3:h:netgear:wnr2050:-:*****:
cpe:2.3:h:netgear:wnr2050:-:*****:
cpe:2.3:o:netgear:wnr2050_firmware:*****:
cpe:2.3:o:netgear:wnr2050_firmware:*****:

No vendor comments have been submitted for this CVE