

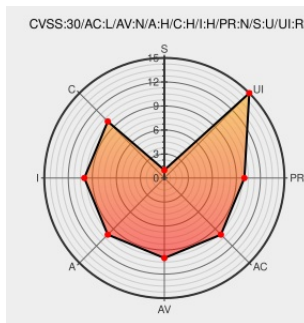


CVE-2017-18742

Published on: 04/23/2020 12:00:00 AM UTC

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

CVE-2017-18742

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

Certain versions of [Jr6150](#) from [Netgear](#) contain the following vulnerability:

Certain NETGEAR devices are affected by CSRF. This affects JR6150 before 1.0.1.10, R6050 before 1.0.1.10, R6250 before 1.0.4.12, R6300v2 before 1.0.4.8, R6700 before 1.0.1.16, R6900 before 1.0.1.16, R7300DST before 1.0.0.54, R7900 before 1.0.1.12, R8000 before 1.0.3.32, and R8500 before 1.0.2.74.

CVE-2017-18742 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Security Advisory for Cross-Site Request Forgery on Some Routers, PSV-2017-0331 Answer NETGEAR Support	Vendor Advisory kb.netgear.com text/html	CONFIRM kb.netgear.com/000051513/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-Routers-PSV-2017-0331

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	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	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	R6250	-	All	All	All
Hardware 	Netgear	R6250	-	All	All	All
Operating System	Netgear	R6250 Firmware	All	All	All	All
Operating System	Netgear	R6250 Firmware	All	All	All	All
Hardware 	Netgear	R6300	v2	All	All	All
Hardware 	Netgear	R6300	v2	All	All	All
Operating System	Netgear	R6300 Firmware	All	All	All	All
Operating System	Netgear	R6300 Firmware	All	All	All	All
Hardware 	Netgear	R6700	-	All	All	All
Hardware 	Netgear	R6700	-	All	All	All
Operating System	Netgear	R6700 Firmware	All	All	All	All
Operating System	Netgear	R6700 Firmware	All	All	All	All
Hardware 	Netgear	R6900	-	All	All	All

Hardware						
Operating System						
Operating System						
Hardware						
Hardware						
Operating System						
Operating System						
Hardware						
Hardware						
Operating System						
Operating System						
Hardware						
Hardware						
Operating System						
Operating System						
Hardware						
Hardware						
Operating System						
Operating System						
Hardware						
Hardware						
Operating System						
Operating System						
Hardware						
Hardware						
Operating System						
Operating System						
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:r6050:-:~::~:						
cpe:2.3:h:netgear:r6050:-:~::~:						
cpe:2.3:o:netgear:r6050_firmware:~::~:						
cpe:2.3:o:netgear:r6050_firmware:~::~:						

```

cpe.2.3.0:netgear:10030_firmware. . . . .

```

```
cpe:2.3:h:netgear:r6250:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:r6250:-:*:*:*:*:*:*:
```

cpe:2.3:o:netgear:r6250_firmware:*:*:*:*:*:*:

```
cpe:2.3:o:netgear:r6250_firmware:*:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:r6300:v2:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:r6300:v2:*:*:*:*:*:*:
```

cpe:2.3:o:netgear:r6300_firmware:*:*:*:*:*:*:*:

```
cpe:2.3:o:netgear:r6300_firmware:*.:.:.:.:.:.:.:
```

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

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

cpe:2.3:o:netgear:r6700_firmware:*:*:*:*:*:*:

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

```
cpe:2.3:h:netgear:r6900:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:r6900:-:*:*:*:*:*:*:
```

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

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

```
cpe:2.3:h:netgear:r7300dst:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:r7300dst:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:netgear:r7300dst_firmware:*:*:*:*:*:*:*:
```

```
cpe:2.3:o:netgear:r7300dst_firmware:*:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:r7900:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:r7900:-:*:*:*:*:*:*:
```

cpe:2.3:o:netgear:r7900_firmware:*.:.:.:.:.:.:.:

cpe:2.3:o:netgear:r7900_firmware:*:*:*:*:*:*:

```
cpe:2.3:h:netgear:r8000:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:r8000:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:netgear:r8000_firmware:*:*:*:*:*:*:*:
```

cpe:2.3:o:netgear:r8000_firmware:*:*:*:*:*:*:

cpe:2.3:h:netgear:r8500:-:*:*:*:*:*:*:
cpe:2.3:h:netgear:r8500:-:*:*:*:*:*:*:
cpe:2.3:o:netgear:r8500_firmware:*:*:*:*:*:*:
cpe:2.3:o:netgear:r8500_firmware:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→