



CVE-2017-18738

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

Last Modified on: 03/23/2021 11:26:56 PM UTC

CVE-2017-18738

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

CVSS:30/AC:L/AV:A/A:H/C:H/I:H/PR:N/S:U/UI:N



Certain versions of [Ex6150](#) from [Netgear](#) contain the following vulnerability:

Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects EX6150v2 before 1.0.1.54, R6400 before 1.0.1.24, R6400v2 before 1.0.2.32, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R7000 before 1.0.9.10, R7000P before 1.2.0.22, R6900P before 1.2.0.22, R7100LG before 1.0.0.32, R7300DST before 1.0.0.54, R7900 before 1.0.1.18, R8000 before 1.0.3.48, R8300 before 1.0.2.106, R8500 before 1.0.2.106, R6100 before 1.0.1.16, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.58.

CVE-2017-18738 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
ADJACENT_NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **5.8 - MEDIUM**

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

CVE References

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

Security Advisory for Pre-Authentication Stack Overflow on
Some Routers and Extenders, PSV-2017-0706 | Answer |
NETGEAR Support

Vendor Advisory
kb.netgear.com
text/html

N CONFIRM kb.netgear.com/000051517/Security-Advisory-for-Pre-Authentication-Stack-Overflow-on-Some-Routers-and-Extenders-PSV-2017-0706

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	Ex6150	v2	All	All	All
Hardware  	Netgear	Ex6150	v2	All	All	All
Operating System	Netgear	Ex6150 Firmware	All	All	All	All
Operating System	Netgear	Ex6150 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	R6400	-	All	All	All
Hardware  	Netgear	R6400	v2	All	All	All
Hardware  	Netgear	R6400	-	All	All	All
Hardware  	Netgear	R6400	v2	All	All	All
Operating System	Netgear	R6400 Firmware	All	All	All	All
Operating System	Netgear	R6400 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  	Netgear	R6900	-	All	All	All
Hardware  	Netgear	R6900p	-	All	All	All
Hardware  	Netgear	R6900p	-	All	All	All
Operating System	Netgear	R6900p Firmware	All	All	All	All
Operating System	Netgear	R6900p Firmware	All	All	All	All
Operating System	Netgear	R6900 Firmware	All	All	All	All
Operating System	Netgear	R6900 Firmware	All	All	All	All
Hardware  	Netgear	R7000	-	All	All	All
Hardware  	Netgear	R7000	-	All	All	All
Hardware  	Netgear	R7000p	-	All	All	All
Hardware  	Netgear	R7000p	-	All	All	All
Operating System	Netgear	R7000p Firmware	All	All	All	All
Operating System	Netgear	R7000p Firmware	All	All	All	All
Operating System	Netgear	R7000 Firmware	All	All	All	All
Operating System	Netgear	R7000 Firmware	All	All	All	All
Hardware  	Netgear	R7100lg	-	All	All	All
Hardware  	Netgear	R7100lg	-	All	All	All
Operating System	Netgear	R7100lg Firmware	All	All	All	All
Operating System	Netgear	R7100lg Firmware	All	All	All	All
Hardware  	Netgear	R7300dst	-	All	All	All
Hardware  	Netgear	R7300dst	-	All	All	All
Operating System	Netgear	R7300dst Firmware	All	All	All	All
Operating System	Netgear	R7300dst Firmware	All	All	All	All
Hardware  	Netgear	R7900	-	All	All	All
Hardware  	Netgear	R7900	-	All	All	All
Operating System	Netgear	R7900 Firmware	All	All	All	All
Operating	Netgear	R7900 Firmware	All	All	All	All

cpe:2.3:o:netgear:ex6150_firmware:*:*:*:*:*:*:

cpe:2.3:o:netgear:ex6150_firmware:*:*:*:*:*:*:

```
cpe:2.3:h:netgear:r6100:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:r6100:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:netgear:r6100_firmware:*:*:*:*:*:*:
```

cpe:2.3:o:netgear:r6100_firmware:*.:.:.:.:.:.:.:

```
cpe:2.3:h:netgear:r6400:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:r6400:v2:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:r6400:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:r6400:v2:*:*:*:*:*:*:
```

```
cpe:2.3:o:netgear:r6400_firmware:*.*.*.*.*.*.*.*
```

cpe:2.3:o:netgear:r6400_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:h:netgear:r6900p:-:*:*:*:*:*:*:

cpe:2.3:h:netgear:r6900p:-:*:*:*:*:*:*:

```
cpe:2.3:o:netgear:r6900p_firmware:*.:.:.:.:.:.:.:
```

cpe:2.3:o:netgear:r6900p_firmware:*:*:*:*:*:*:

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

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

```
cpe:2.3:h:netgear:r7000:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:r7000:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:r7000p:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:netgear:r7000p:-:*:*:*:*:*:
```

0000070000 *****

cpe:2.3:o:netgear:r7000p_firmware:*****:
cpe:2.3:o:netgear:r7000p_firmware:*****:
cpe:2.3:o:netgear:r7000_firmware:*****:
cpe:2.3:o:netgear:r7000_firmware:*****:
cpe:2.3:h:netgear:r7100lg:-:*****:
cpe:2.3:h:netgear:r7100lg:-:*****:
cpe:2.3:o:netgear:r7100lg_firmware:*****:
cpe:2.3:o:netgear:r7100lg_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:r8300:-:*****:
cpe:2.3:h:netgear:r8300:-:*****:
cpe:2.3:o:netgear:r8300_firmware:*****:
cpe:2.3:o:netgear:r8300_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:*****:
cpe:2.3:h:netgear:wndr4300:v2.*****:

cpe:2.3:h:netgear:wndr4300:v2:*****:
cpe:2.3:o:netgear:wndr4300_firmware:*****:
cpe:2.3:o:netgear:wndr4300_firmware:*****:
cpe:2.3:h:netgear:wndr4500:v3:*****:
cpe:2.3:h:netgear:wndr4500:v3:*****:
cpe:2.3:o:netgear:wndr4500_firmware:*****:
cpe:2.3:o:netgear:wndr4500_firmware:*****:
cpe:2.3:h:netgear:wnr2000:v5:*****:
cpe:2.3:h:netgear:wnr2000:v5:*****:
cpe:2.3:o:netgear:wnr2000_firmware:*****:
cpe:2.3:o:netgear:wnr2000_firmware:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)