



CVE-2020-15636

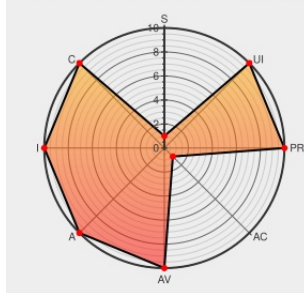
Published on: 08/19/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:41 PM UTC

CVE-2020-15636

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

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



Certain versions of **R6700** from **Netgear** contain the following vulnerability:

This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR R6400, R6700, R7000, R7850, R7900, R8000, RS400, and XR300 routers with firmware 1.0.4.84_10.0.58. Authentication is not required to exploit this vulnerability. The specific flaw exists within the check_ra service. A crafted raePolicyVersion in a RAE_Policy.json file can trigger an overflow of a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9852.

CVE-2020-15636 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **NETGEAR - Multiple Routers** version **1.0.4.84_10.0.58**

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **10 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description

Tags

Link

Security Advisory for Pre-Authentication Stack Overflow on R6700v3, PSV-2020-0224 | Answer | NETGEAR Support

Vendor Advisory

kb.netgear.com

text/html

N

MISC kb.netgear.com/000062128/Security-Advisory-for-Pre-Authentication-Stack-Overflow-on-R6700v3-PSV-2020-0224

ZDI-20-937 | Zero Day Initiative

Third Party Advisory

VDB Entry

www.zerodayinitiative.com

text/html

Z

MISC www.zerodayinitiative.com/advisories/ZDI-20-937/

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

R6700

v3

All

All

All

Hardware  

Netgear

R6700

v3

All

All

All

Operating System

Netgear

R6700 Firmware

All

All

All

All

Operating System

Netgear

R6700 Firmware

All

All

All

All

cpe:2.3:h:netgear:r6700:v3:*****:

cpe:2.3:h:netgear:r6700:v3:*****:

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

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

Discovery Credit

Pedro Ribeiro (@pedrib1337 | pedrib@gmail.com) and Radek Domanski (@RabbitPro | radek.domanski@gmail.com)

← Previous ID

Next ID →

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](#)