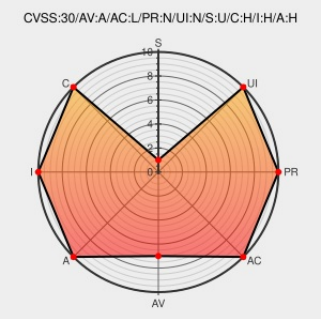
CVE-2020-15635

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

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

CVE-2020-15635

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of R6700 from Netgear contain the following vulnerability:

This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers with firmware 1.0.4.84_10.0.58. Authentication is not required to exploit this vulnerability. The specific flaw exists within the acsd service, which listens on TCP port 5916 by default. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the admin user. Was ZDI-CAN-9853.

CVE-2020-15635 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **NETGEAR** - **R6700** version **1.0.4.84_10.0.58**

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: 8.3 - HIGH

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Security Advisory for Pre-Authentication Buffer Overflow on R6700v3, PSV-2020-0202 | Answer | NETGEAR Support	Vendor Advisory kb.netgear.com text/html	MISC kb.netgear.com/000062127/Security-Advisory-for-Pre-Authentication-Buffer-Overflow-on-R6700v3-PSV-2020-0202
ZDI-20-936 | Zero Day Initiative	Third Party Advisory VDB Entry www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-20-936/

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.report 2023 |
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 registred 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