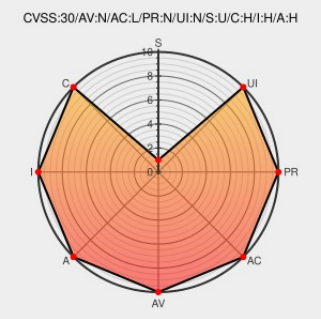
CVE-2019-11560

Published on: 05/07/2019 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2019-11560

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



Certain versions of Hi3516 from Hisilicon contain the following vulnerability:

A buffer overflow vulnerability in the streaming server provided by hisilicon in HI3516 models allows an unauthenticated attacker to remotely run arbitrary code by sending a special RTSP over HTTP packet. The vulnerability was found in many cameras using hisilicon's hardware and software, as demonstrated by TENVIS cameras 1.3.3.3, 1.2.7.2, 1.2.1.4, 7.1.20.1.2, and 13.1.1.1.7.2; FDT FD7902 11.3.14.1.3 and 10.3.14.1.3; FOSCAM cameras 3.2.1.1.1_0815 and 3.2.2.2.1_0815; and Dericam cameras V11.3.8.1.12.

CVE-2019-11560 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

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
Vulnerability found in hisilicon HI3516	Third Party Advisory	MISC

Vulnerability found in hisilicon Hi3516 · GitHub	Third Party Advisory gist.github.com text/html	MISC gist.github.com/vulnfan1337/e95c2dba75ad93a1a325c6ace950eba9

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	Hisilicon	Hi3516	-	All	All	All
Hardware	Hisilicon	Hi3516	-	All	All	All
Operating System	Hisilicon	Hi3516 Firmware	-	All	All	All
Operating System	Hisilicon	Hi3516 Firmware	-	All	All	All

cpe:2.3:h:hisilicon:hi3516:-:*:*:*:*:*:*:*:

cpe:2.3:h:hisilicon:hi3516:-:*:*:*:*:*:*:*:

cpe:2.3:o:hisilicon:hi3516_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:o:hisilicon:hi3516_firmware:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← 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