



CVE-2019-10711

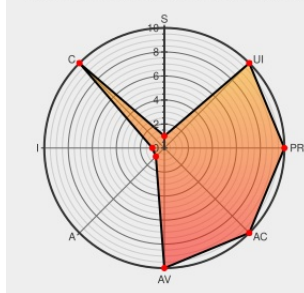
Published on: 04/23/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:40 PM UTC

CVE-2019-10711

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

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



Certain versions of [Hi3510](#) from [Hisilicon](#) contain the following vulnerability:

Incorrect access control in the RTSP stream and web portal on all IP cameras based on Hisilicon Hi3510 firmware (until Webware version V1.0.1) allows attackers to view an RTSP stream by connecting to the stream with hidden credentials (guest or user) that are neither displayed nor configurable in the camera's CamHi or keye mobile

management application. This affects certain devices labeled as HI3510, HI3518, LOOSAFE, LEVCOECAM, Sywstoda, BESDER, WUSONGLUSAN, GADINAN, Unitoptek, ESCAM, etc.

CVE-2019-10711 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
BullGuard 2021: 1 Antivirus and VPN for your home and	This Post Antivirus	MISC deia bullguard.com/deia-by

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Hisilicon	Hi3510	-	All	All	All
Hardware 	Hisilicon	Hi3510	-	All	All	All
Operating System	Hisilicon	Hi3510 Firmware	All	All	All	All
Operating System	Hisilicon	Hi3510 Firmware	All	All	All	All
<pre>cpe:2.3:h:hisilicon:hi3510:-:*:*:*:*:*.*</pre>						
<pre>cpe:2.3:h:hisilicon:hi3510:-:*:*:*:*:*.*</pre>						
<pre>cpe:2.3:o:hisilicon:hi3510_firmware:*:*:*:*:*.*</pre>						
<pre>cpe:2.3:o:hisilicon:hi3510_firmware:*:*:*:*:*.*</pre>						