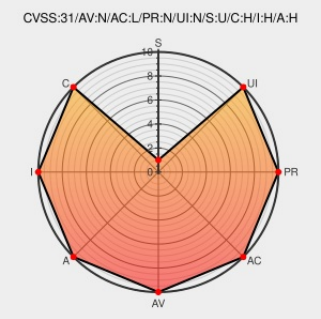
CVE-2020-9527

Published on: 08/10/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:15 PM UTC

CVE-2020-9527

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



Certain versions of Shenzhen Hichip Vision Technology Firmware from Hichip contain the following vulnerability:

Firmware developed by Shenzhen Hichip Vision Technology (V6 through V20, after 2018-08-09 through 2020), as used by many different vendors in millions of Internet of Things devices, suffers from buffer overflow vulnerability that allows unauthenticated remote attackers to execute arbitrary code via the peer-to-peer (P2P) service. This affects products marketed under the following brand names: Accfly, Alptop, Anlink, Besdersec, BOAVISION, COOAU, CPVAN, Ctronics, D3D Security, Dericam, Elex System, Elite Security, ENSTER, ePGes, Escam, FLOUREON, GENBOLT, Hongjingtian (HJT), ICAMI, Iegeek, Jecurity, Jennov, KKMoon, LEFTEK, Loosafe, Luowice, Nesuniq, Nettoly, ProElite, QZT, Royallite, SDETER, SV3C, SY2L, Tenvis, ThinkValue, TOMLOV, TPTEK, WGCC, and ZILINK.

CVE-2020-9527 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: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Security cameras vulnerable to hijacking	Not Applicable hacked.camera text/html	MISC hacked.camera/
Security cameras vulnerable to hijacking	Not Applicable redprocyon.com text/html	MISC redprocyon.com

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
Operating System	Hichip	Shenzhen Hichip Vision Technology Firmware	All	All	All	All
Operating System	Hichip	Shenzhen Hichip Vision Technology Firmware	All	All	All	All

cpe:2.3:o:hichip:shenzhen_hichip_vision_technology_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:hichip:shenzhen_hichip_vision_technology_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→