



CVE-2020-9529

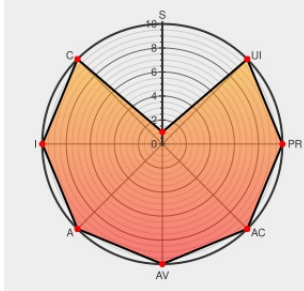
Published on: 08/10/2020 12:00:00 AM UTC

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

CVE-2020-9529

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Shenzhen Hichip Vision Technology Firmware](#) from [Hichip](#) contain the following vulnerability:

Firmware developed by Shenzhen Hichip Vision Technology (V6 through V20), as used by many different vendors in millions of Internet of Things devices, suffers from a privilege escalation vulnerability that allows attackers on the local network to reset the device's administrator password. 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, Igeek, Jecurity, Jennov, KKMoon, LEFTEK, Loosafe, Luowice, Nesuniq, Nettoly, ProElite, QZT, Royallite, SDETER, SV3C, SY2L, Tervis, ThinkValue, TOMLOV, TPTEK, WGCC, and ZILINK.

CVE-2020-9529 has been assigned by [M](#) [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

Security cameras vulnerable to hijacking

Tags

Not Applicable

hacked.camera

text/html

Link

 [MISC hacked.camera/](#)

Description

Security cameras vulnerable to hijacking

Tags

Not Applicable

redprocyon.com

text/html

Link

 [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

Social Mentions

Source	Title	Posted (UTC)
 @fercorvalan	@ALoosafe I need information about firmware update of Loosafe LS-F2-T and vulnerability CVE-2020-9529 and others (... twitter.com/i/web/status/1...	2021-03-27 04:06:57

← Previous ID

Next ID →