



Published on: 05/23/2019 12:00:00 AM UTC

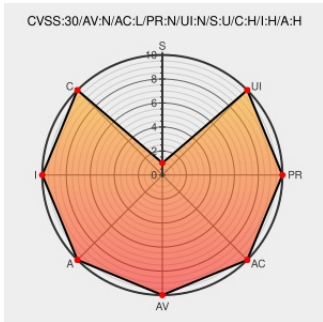
Last Modified on: 03/23/2021 11:27:41 PM UTC

CVE-2019-12289

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of C38s from Vstracam contain the following vulnerability:

An issue was discovered in upgrade_firmware.cgi on VStarcam 100T (C7824WIP) CH-sys-48.53.75.119~123 and 200V (C38S) CH-sys-48.53.203.119~123 devices. A remote command can be executed through a system firmware update without authentication. The attacker can modify the files within the internal firmware or even steal account information by executing a command.

CVE-2019-12289 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
S/W	Broken Link f1security.co.kr	MISC f1security.co.kr/cve/cve_190314.htm

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 🇹🇼 ↗️	Vstracam	C38s	-	All	All	All
Hardware 🇹🇼 ↗️	Vstracam	C38s	-	All	All	All
Operating System	Vstracam	C38s Firmware	ch-sys-48.53.203.119\~123	All	All	All
Operating System	Vstracam	C38s Firmware	ch-sys-48.53.203.119~123	All	All	All
Operating System	Vstracam	C38s Firmware	ch-sys-48.53.203.119\~123	All	All	All
Hardware 🇹🇼 ↗️	Vstracam	C7824wip	-	All	All	All
Hardware 🇹🇼 ↗️	Vstracam	C7824wip	-	All	All	All
Operating System	Vstracam	C7824wip Firmware	ch-sys-48.53.75.119\~123	All	All	All
Operating System	Vstracam	C7824wip Firmware	ch-sys-48.53.75.119~123	All	All	All
Operating System	Vstracam	C7824wip Firmware	ch-sys-48.53.75.119\~123	All	All	All
cpe:2.3:h:vstracam:c38s:-:*:*:*:*:*:						
cpe:2.3:h:vstracam:c38s:-:*:*:*:*:*:						
cpe:2.3:o:vstracam:c38s_firmware:ch-sys-48.53.203.119\~123:*:*:*:*:*:						
cpe:2.3:o:vstracam:c38s_firmware:ch-sys-48.53.203.119~123:*:*:*:*:*:						
cpe:2.3:o:vstracam:c38s_firmware:ch-sys-48.53.203.119\~123:*:*:*:*:*:						
cpe:2.3:h:vstracam:c7824wip:-:*:*:*:*:*:						
cpe:2.3:h:vstracam:c7824wip:-:*:*:*:*::~:						
cpe:2.3:o:vstracam:c7824wip_firmware:ch-sys-48.53.75.119\~123:*:*:*:*:*:						
cpe:2.3:o:vstracam:c7824wip_firmware:ch-sys-48.53.75.119~123:*:*:*:*::~:						
cpe:2.3:o:vstracam:c7824wip_firmware:ch-sys-48.53.75.119\~123:*:*:*:*::~:						

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 registered 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](#)