



CVE-2022-38399

Published on: Not Yet Published

Last Modified on: 09/15/2022 10:23:00 PM UTC

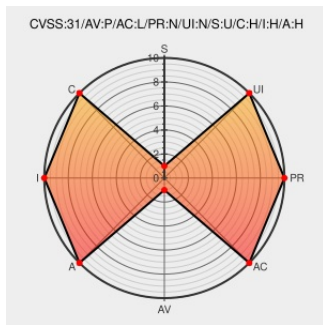
CVE-2022-38399

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Cs-qr10](#) from [Planex](#) contain the following vulnerability:

Missing protection mechanism for alternate hardware interface in SmaCam CS-QR10 all versions and SmaCam Night Vision CS-QR20 all versions allows an attacker to execute an arbitrary OS command by having the product connect to the product's specific serial connection

CVE-2022-38399 has been assigned by [vultures@jpcert.or.jp](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [PLANEX COMMUNICATIONS INC.](#) - [SmaCam CS-QR10](#) and [SmaCam Night Vision CS-QR20](#) version **All versions**

CVSS3 Score: **6.8 - MEDIUM**

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



CVE References

Description	Tags	Link
No Description Provided	www.planex.co.jp text/html	MISC www.planex.co.jp/products/cs-qr10/index.shtml
JVNVU#90766406: Multiple vulnerabilities in PLANEX Network camera products	jvn.jp text/xml	MISC jvn.jp/en/vu/JVNVU90766406/index.html
No Description Provided	www.planex.co.jp text/html	MISC www.planex.co.jp/products/cs-qr20/index.shtml

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

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Planex	Cs-qr10	-	All	All	All
Operating System	Planex	Cs-qr10 Firmware	All	All	All	All
Hardware 	Planex	Cs-qr20	-	All	All	All
Operating System	Planex	Cs-qr20 Firmware	All	All	All	All
<code>cpe:2.3:h:planex:cs-qr10:-:*:*:*:*:*:</code>						
<code>cpe:2.3:o:planex:cs-qr10_firmware:*:*:*:*:*:</code>						
<code>cpe:2.3:h:planex:cs-qr20:-:*:*:*:*:*:</code>						
<code>cpe:2.3:o:planex:cs-qr20_firmware:*:*:*:*:*:</code>						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVereport	CVE-2022-38399 : Missing protection mechanism for alternate hardware interface in SmaCam CS-QR10 all versions and S... twitter.com/i/web/status/1...	2022-09-08 07:17:47
 /r/netcve	CVE-2022-38399	2022-09-08 07:38:22

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2022   |

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