



CVE-2022-2661

Published on: Not Yet Published

Last Modified on: 06/28/2023 02:20:00 PM UTC

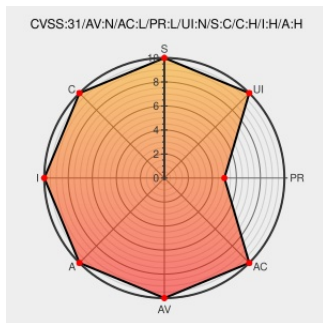
CVE-2022-2661

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Portbloque S** from **Sequi** contain the following vulnerability:

Sequi PortBloque S has an improper authorization vulnerability, which may allow a low-privileged user to perform administrative functions using specifically crafted requests.

CVE-2022-2661 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Sequi - PortBloque S** version = **All**

Vulnerability Patch/Work Around

Minimize network exposure for all control system devices and/or systems, and ensure they are not accessible from the Internet. Locate control system networks and remote devices behind firewalls and isolate them from business networks. When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its connected devices.

CVSS3 Score: **8.8 - HIGH**

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

CVE References

Description	Tags	Link
Sequi PortBloque S CISA	www.cisa.gov text/html	MISC www.cisa.gov/uscert/ics/advisories/icsa-22-228-07

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 purposes. CVEreport does not necessarily endorse the views expressed, or agree with the facts presented on these sites. Further

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 	Sequi	Portbloque S	-	All	All	All
Operating System	Sequi	Portbloque S Firmware	All	All	All	All
cpe:2.3:h:sequi:portbloque_s:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:sequi:portbloque_s_firmware:~::~~::~~::~~::~~::~~::~~::						

Discovery Credit

Byron Chaney of Accenture Security reported these vulnerabilities to CISA.

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-2661 : Sequi PortBloque S has an improper authorization vulnerability, which may allow a low-privileged us... twitter.com/i/web/status/1...	2022-08-16 21:10:26
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-2661 Sequi PortBloque S has an improper authorization vulnerability, wh... twitter.com/i/web/status/1...	2022-08-16 21:55:55

[← 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](#)