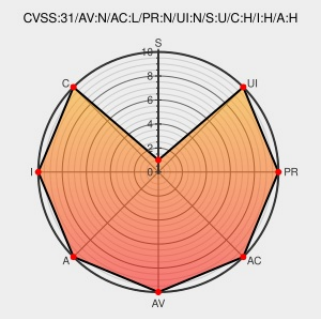
CVE-2022-2103

Published on: Not Yet Published

Last Modified on: 07/05/2022 05:05:00 PM UTC

CVE-2022-2103 - advisory for ICSA-22-174-03

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



Certain versions of Sepcos Control And Protection Relay from Secheron contain the following vulnerability:

An attacker with weak credentials could access the TCP port via an open FTP port, allowing an attacker to read sensitive files and write to remotely executable directories.

CVE-2022-2103 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Secheron** - **SEPCOS Control and Protection Relay firmware package** version **< 1.23.21**

Affected Vendor/Software: **Secheron** - **SEPCOS Control and Protection Relay firmware package** version **< 1.24.8**

Affected Vendor/Software: **Secheron** - **SEPCOS Control and Protection Relay firmware package** version **< 1.25.3**

Vulnerability Patch/Work Around

Additional workarounds are suggested to help reduce the risk: Configure the network such that PLC communications are strictly limited to only the devices required to perform its functions. Limit remote access and close Ports 80 and 443 at the switch level. Only use approved devices to connect to the PLCs. Do not connect personal peripherals (USB sticks, hotspots) to approved devices. Check device logs during periodic maintenance for unauthorized changes or access.

CVSS3 Score: 9.1 - CRITICAL

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

CVSS2 Score: 6.4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Secheron SEPCOS Control and Protection Relay | CISA	www.cisa.gov text/html	MISC www.cisa.gov/uscert/ics/advisories/icsa-22-174-03

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	Secheron	Sepcos Control And Protection Relay	-	All	All	All
Operating System	Secheron	Sepcos Control And Protection Relay Firmware	All	All	All	All

cpe:2.3:h:secheron:sepcos_control_and_protection_relay:-:*:*:*:*:*:*:*:

cpe:2.3:o:secheron:sepcos_control_and_protection_relay_firmware:*:*:*:*:*:*:*:*:

Discovery Credit

Anthony Candarini of AECOM, Clark Bradley of Elliott Davis, Mike Curnow of AECOM, and Balakrishna Subramoney of SAM Analytic Solutions reported these vulnerabilities to CISA.

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-2103 : An attacker with weak credentials could access the TCP port via an open FTP port, allowing an attac… twitter.com/i/web/status/1…	2022-06-24 15:16:23
/r/netcve	CVE-2022-2103	2022-06-24 16:38:08

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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