

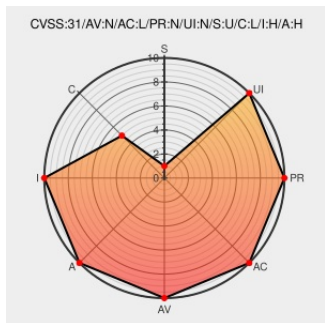


CVE-2022-2102

Published on: Not Yet Published

Last Modified on: 07/06/2022 12:46:00 PM UTC

CVE-2022-2102 - advisory for ICSA-22-174-03

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

Certain versions of [Sepecos Control And Protection Relay](#) from [Secheron](#) contain the following vulnerability:

Controls limiting uploads to certain file extensions may be bypassed. This could allow an attacker to intercept the initial file upload page response and modify the associated code. This modified code can be forwarded and used by a script loaded later in the sequence, allowing for arbitrary file upload into a location where PHP scripts may be

executed.

CVE-2022-2102 has been assigned by [ics-cert@hq.dhs.gov](#) to track the vulnerability - currently rated as **HIGH** 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: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

Access

Access

Authentication

Vector	Complexity	
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	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-2022-2102 : Controls limiting uploads to certain file extensions may be bypassed. This could allow an attacker... twitter.com/i/web/status/1...	2022-06-24 15:16:02
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-2102 Controls limiting uploads to certain file extensions may be bypass... twitter.com/i/web/status/1...	2022-06-24 16:55:55
 @LinInfoSec	Php - CVE-2022-2102: cisa.gov/uscert/ics/adv...	2022-06-24 17:00:17
 /r/netcve	CVE-2022-2102	2022-06-24 16:38:07

© [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](#)