



CVE-2021-33842

Published on: 06/09/2021 12:00:00 AM UTC

Last Modified on: 10/25/2022 11:40:00 PM UTC

CVE-2021-33842 - advisory for INCIBE-2021-0228

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

CVSS:31/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



Certain versions of [Sge-plc1000](#) from [Circutor](#) contain the following vulnerability:

Improper Authentication vulnerability in the cookie parameter of Circutor SGE-PLC1000 firmware version 0.9.2b allows an attacker to perform operations as an authenticated user. In order to exploit this vulnerability, the attacker must be within the network where the device affected is located.

CVE-2021-33842 has been assigned by cve-coordination@incibe.es to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Circutor - SGE-PLC1000** version = **0.9.2b**

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **7.7 - HIGH**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Circutor SGE-PLC1000 improper	www.incibe-cert.es	CONFIRM www.incibe-cert.es/en/early-warning/ics-

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 	Circutor	Sge-plc1000	-	All	All	All
Operating System	Circutor	Sge-plc1000 Firmware	0.9.2b	All	All	All
cpe:2.3:h:circutor:sge-plc1000:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:o:circutor:sge-plc1000_firmware:0.9.2b:~::~~::~~::~~::~~::~~::~~::						

Discovery Credit

Industrial Cybersecurity team of S21sec, special mention to Aarón Flecha Menéndez.

Social Mentions

Source	Title	Posted (UTC)
 @incibe_cert	⚠ Autenticación incorrecta en SGE-PLC1000 de #Circutor #SCI #CNA #ZeroDay #CVE CVE-2021-33842 incibe-cert.es/alerta-tempran...	2021-06-08 09:14:55
 @incibe_cert	⚠ Autenticación incorrecta en SGE-PLC1000 de #Circutor #SCI #CNA #ZeroDay #CVE CVE-2021-33842 incibe-cert.es/alerta-tempran...	2021-06-09 10:33:06
 @CVEreport	CVE-2021-33842 : Improper Authentication vulnerability in the cookie parameter of Circutor SGE-PLC1000 firmware ver... twitter.com/i/web/status/1...	2021-06-09 12:09:19
 /r/netcve	CVE-2021-33842	2021-06-09 12:41:37

[← 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](#)