



CVE-2021-39190

Published on: Not Yet Published

Last Modified on: 09/26/2022 02:02:00 PM UTC

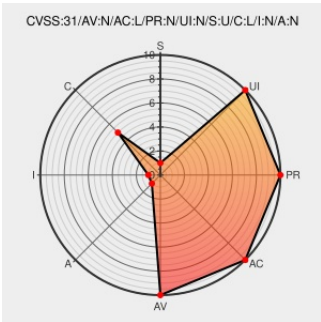
CVE-2021-39190 - advisory for GHSA-3324-57w6-jxcq

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [System Center Configuration Manager](#) from [Teclib-edition](#) contain the following vulnerability:

The SCCM plugin for GLPI is a plugin to synchronize computers from SCCM (version 1802) to GLPI. In versions prior to 2.3.0, the Configuration page is publicly accessible in read-only mode. This issue is patched in version 2.3.0. No known workarounds exist.

CVE-2021-39190 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [pluginsGLPI](#) - `sccm` version < 2.3.0

CVSS3 Score: **5.3 - MEDIUM**

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

CVE References

Description	Tags	Link
Merge pull request from GHSA-3324-57w6-jxcq · pluginsGLPI/sccm@29a7f92 · GitHub	github.com text/html	MISC github.com/pluginsGLPI/sccm/commit/29a7f92d32a0cf9aa3f22c52c50b738274d2813e
Configuration page is accessible publicly (read only) · Advisory · pluginsGLPI/sccm · GitHub	github.com text/html	CONFIRM github.com/pluginsGLPI/sccm/security/advisories/GHSA-3324-57w6-jxcq

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
Application	Teclib-edition	System Center Configuration Manager	All	All	All	All
cpe:2.3:a:teclib-edition:system_center_configuration_manager:*:*:*:*:*:gli:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-39190 : The SCCM plugin for GLPI is a plugin to synchronize computers from SCCM version 1802 to GLPI. In... twitter.com/i/web/status/1...	2022-09-22 16:34:55
 @JohnJasonFallow	New vulnerability on the NVD: CVE-2021-39190 ift.tt/cPeYzUa	2022-09-22 18:16:17
 @doogsineerg	New vulnerability on the NVD: CVE-2021-39190 ift.tt/dETYu32	2022-09-22 18:33:01
 @workentin	New vulnerability on the NVD: CVE-2021-39190 ift.tt/J4HA0fm	2022-09-22 18:40:37
 @xanadulinux	CVE-2021-39190 ift.tt/lflQrKD	2022-09-22 18:52:31
 @4ng3n01r3	#CyberSecurity #Security #CERT #CVE #Nist #breach #vulnerability : CVE-2021-39190	2022-09-22 18:55:05
 /r/netcve	CVE-2021-39190	2022-09-22 17:38:28

[← 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](#)