



CVE-2021-21905

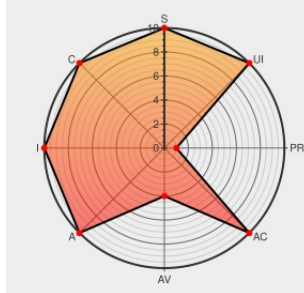
Published on: 12/22/2021 12:00:00 AM UTC

Last Modified on: 08/31/2022 07:12:00 PM UTC

CVE-2021-21905

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

CVSS:30/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H



Certain versions of [Ic Module Cma](#) from [Garrett](#) contain the following vulnerability:

Stack-based buffer overflow vulnerability exists in how the CMA readfile function of Garrett Metal Detectors iC Module CMA Version 5.0 is used at various locations. The Garrett iC Module exposes an authenticated CLI over TCP port 6877. This interface is used by a secondary GUI client, called “CMA Connect”, to interact with the iC Module on behalf of the user. After a client successfully authenticates, they can send plaintext commands to manipulate the device.

CVE-2021-21905 has been assigned by [Cisco Talos](#) talos-cna@cisco.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.2 - HIGH**

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

CVSS2 Score: **8.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
TALOS-2021-1357 Cisco Talos Intelligence Group	CVE-2021-21905	MISC

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
Operating System	Garrett	Ic Module Cma	5.0	All	All	All
cpe:2.3:o:garrett:ic_module_cma:5.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

[← Previous ID](#)

[Next ID →](#)