



CVE-2023-5222

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-5222
State	PUBLIC
Assigner	cna@vuldb.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-27 15:19:00 UTC
Updated	2023-11-07 04:23:00 UTC
Description	A vulnerability classified as critical was found in Viessmann Vitogate 300 up to 2.1.3.0. This vulnerability affects the function

Risk And Classification

Problem Types: CWE-259

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Viessmann	Vitogate 300	-	All	All	All
Operating System	Viessmann	Vitogate 300 Firmware	All	All	All	All

References

Reference	Source	Link
Information	MISC	github.cc
Login required	MISC	vuldb.co
CVE-2023-5222: Viessmann Vitogate 300 Web Management Interface vitogate.cgi isValidUser hard-coded password	MISC	vuldb.co
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report