



CVE-2022-38100

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

Summary

CVE	CVE-2022-38100
State	PUBLIC
Assigner	ics-cert@hq.dhs.gov
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-13 15:15:00 UTC
Updated	2023-07-21 20:05:00 UTC
Description	The CMS800 device fails while attempting to parse malformed network data sent by a threat actor. A threat actor with network access to the device can exploit this vulnerability to cause a denial of service. The vulnerability is caused by a buffer overflow in the CMS800 device's network stack. The vulnerability is caused by a buffer overflow in the CMS800 device's network stack. The vulnerability is caused by a buffer overflow in the CMS800 device's network stack.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Contechealth	Cms8000	-	All	All	All
Operating System	Contechealth	Cms8000 Firmware	-	All	All	All

References

Reference	Source	Link	Tags
Contec Health CMS8000 CISA	MISC	www.cisa.gov	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Level Nine reported these vulnerabilities to CISA.

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