



CVE-2022-3027

Published on: Not Yet Published

Last Modified on: 09/14/2022 10:42:00 PM UTC

CVE-2022-3027 - advisory for ICSMA-22-244-01

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

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



Certain versions of [Cms8000](#) from [Contechealth](#) contain the following vulnerability:

The CMS8000 device does not properly control or sanitize the SSID name of a new Wi-Fi access point. A threat actor could create an SSID with a malicious name, including non-standard characters that, when the device attempts connecting to the malicious SSID, the device can be exploited to write arbitrary files or display incorrect information.

CVE-2022-3027 has been assigned by [ics-cert@hq.dhs.gov](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Contec Health](#) - **CMS8000 CONTEC ICU CCU Vital Signs Patient Monitor** version = **All**

Vulnerability Patch/Work Around

Contec Health has not responded to requests to work with CISA to mitigate these vulnerabilities. Users of these affected products are invited to contact Contec Health for additional information. The following mitigations could assist in reducing the risk for exploitation of vulnerabilities: Disabling UART functionality at the CPU level Enforcing unique device authentication before granting access to the terminal / bootloader Where possible, enforcing secure boot. Tamper stickers on the device casing to indicate when a device has been opened

CVSS3 Score: **5.7 - MEDIUM**

Attack
Vector

Attack
Complexity

Privileges
Required

User
Interaction

ADJACENT_NETWORK

LOW

NONE

REQUIRED

Scope

Confidentiality
Impact

Integrity
Impact

Availability
Impact

UNCHANGED

NONE

HIGH

NONE

CVE References

Description

Tags

Link

Contec Health CMS8000 | CISA

[www.cisa.gov
text/html](https://www.cisa.gov/text/html)

[MISC www.cisa.gov/uscert/ics/advisories/icsma-22-244-01](https://www.cisa.gov/uscert/ics/advisories/icsma-22-244-01)

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 	Contechealth	Cms8000	-	All	All	All
Operating System	Contechealth	Cms8000 Firmware	-	All	All	All
cpe:2.3:h:contechealth:cms8000:-:*:*:*:*:*:						
cpe:2.3:o:contechealth:cms8000_firmware:-:*:*:*:*:*:						

Discovery Credit

Level Nine reported these vulnerabilities to CISA.

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-3027 : The CMS8000 device does not properly control or sanitize the SSID name of a new Wi-Fi access point.... twitter.com/i/web/status/1...	2022-09-13 15:05:14

[← 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](#)