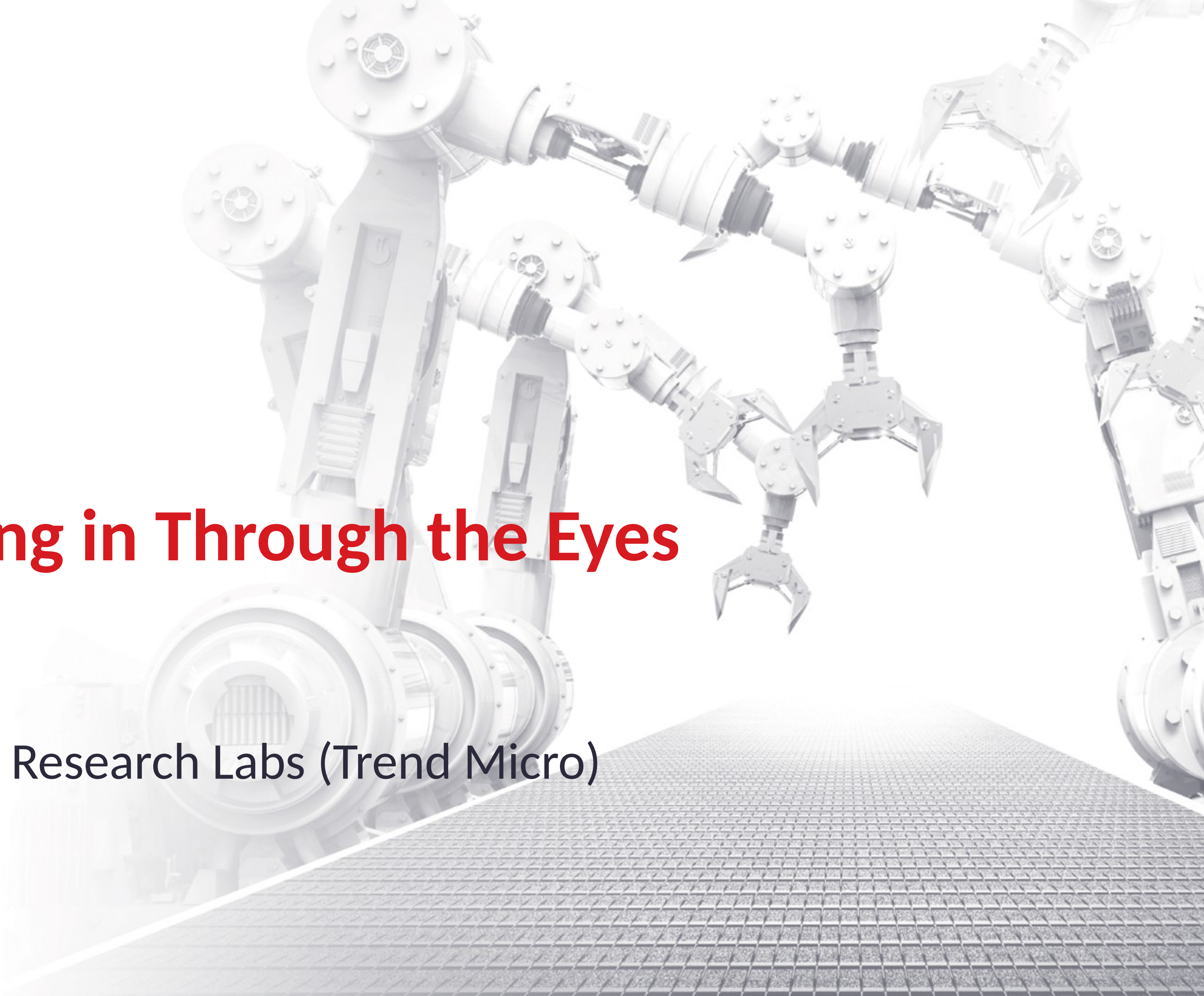
txOne™ networks



Pwning OT: Going in Through the Eyes

Ta-Lun Yen

TXOne IoT/ICS Security Research Labs (Trend Micro)

$(whoami)

- @evanslify
- Threat Researcher @ TXOne Networks (Trend Micro), 2019/11-present
- Focused on reverse engineering, protocol analysis, wireless, hardware
  - Apple proprietary protocol
- Previously: BHEU 2019, HITCON

Outline

- Introduction
- Approach
- Security analysis *without actual hardware*
- Results
- Demo
- Future Work

Introduction

- Human Machine Interface

Introduction

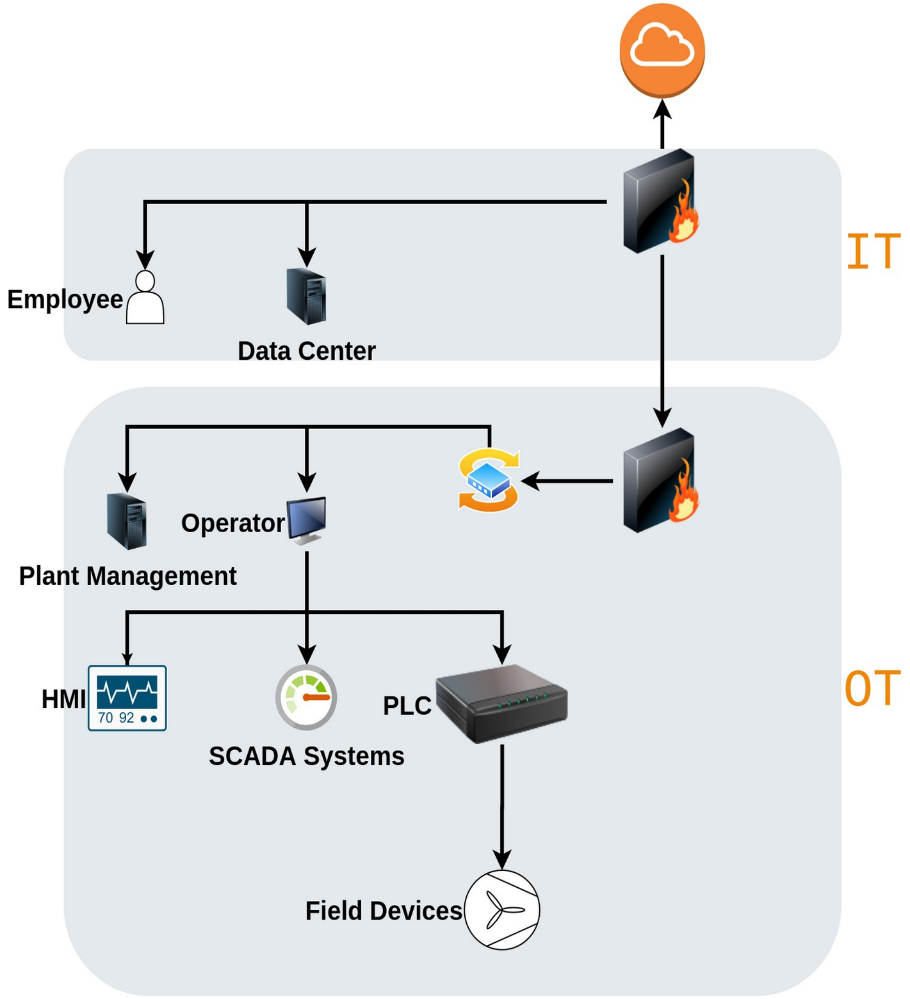
- Human Machine Interface

Introduction

- HMI
  - Cyber-physical interaction
    - Start/stop cycle
    - Interact with control process
  - Data visualization
    - Visible representation of output states (e.g. sensors)

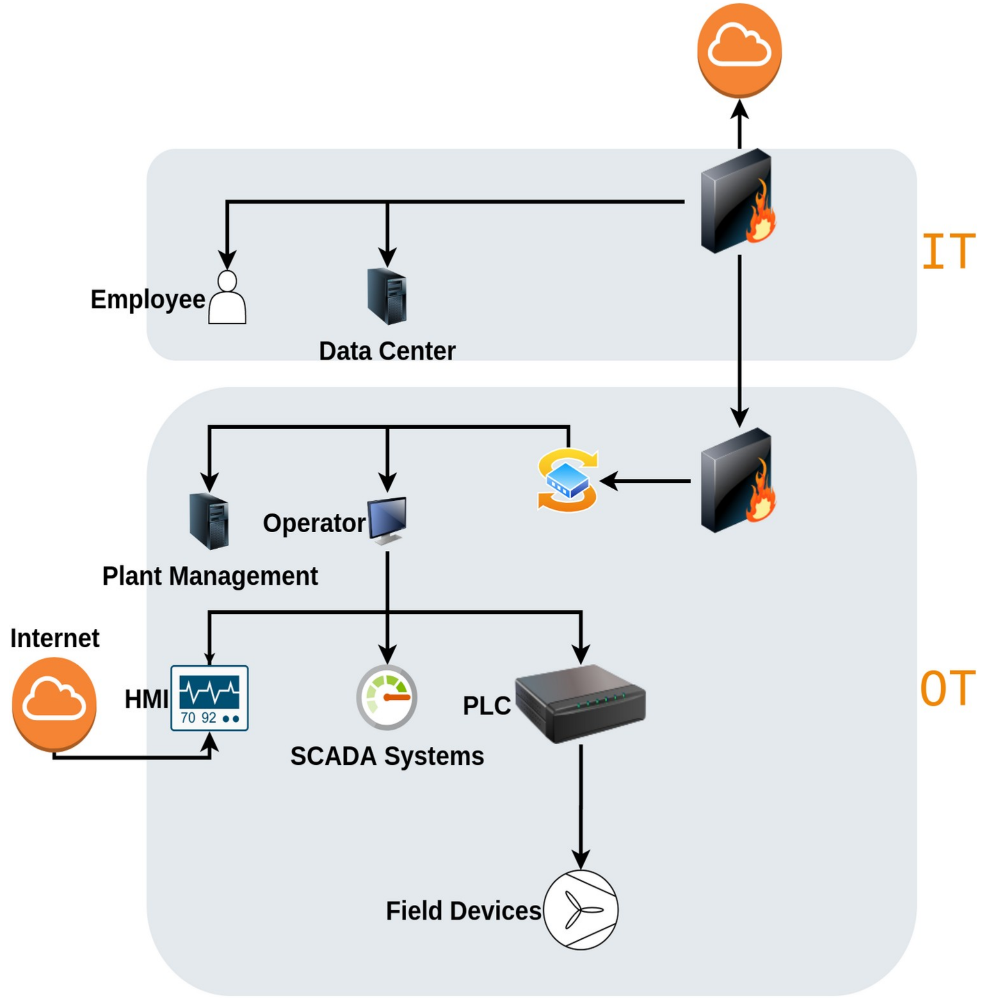
Introduction

- How HMI is placed in a network
  - In a wonderful world, everything would be wonderfully segmented!
  - However, things are not as wonderful as we might hope



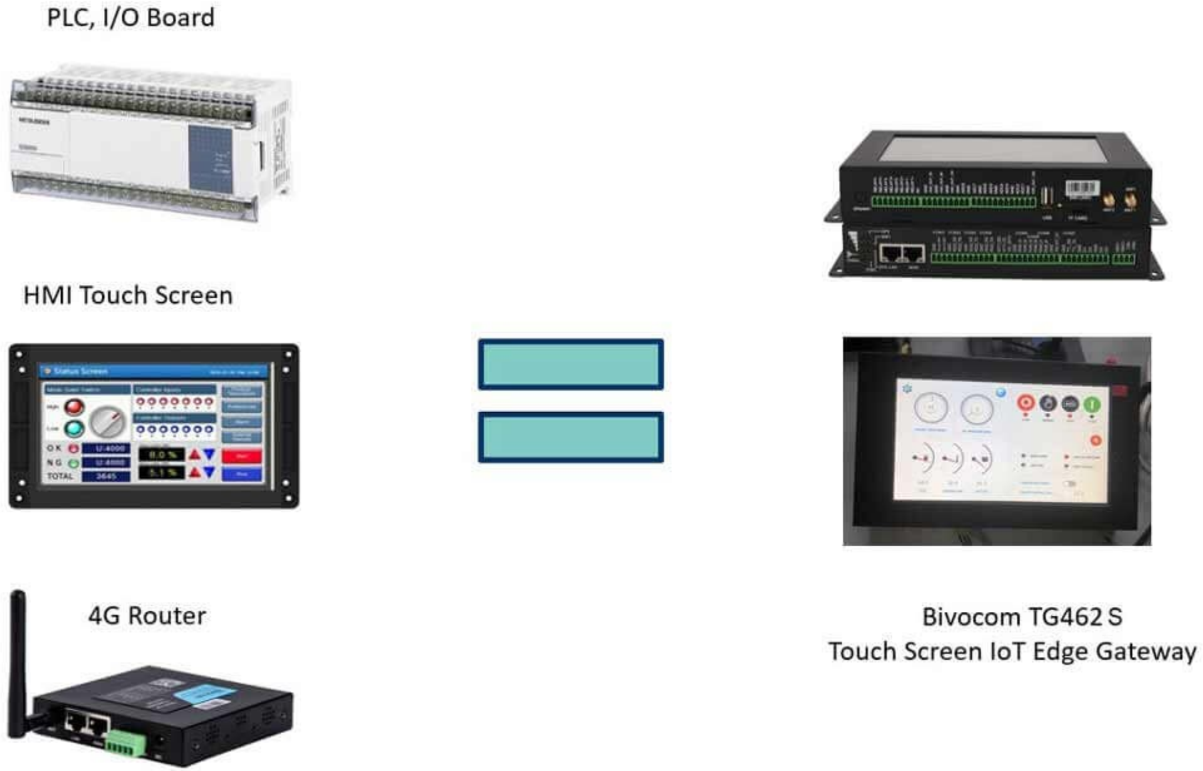
Introduction

- How HMI is placed in a network
  - – ... In fact, they are sometimes much worse!



Introduction

- In some cases
  - HMI could be installed as a runtime and run on general-purpose PC
    - Siemens WinCC, mySCADA…
  - Some vendors even combined LTE Gateway and HMI!



PLC, I/O Board

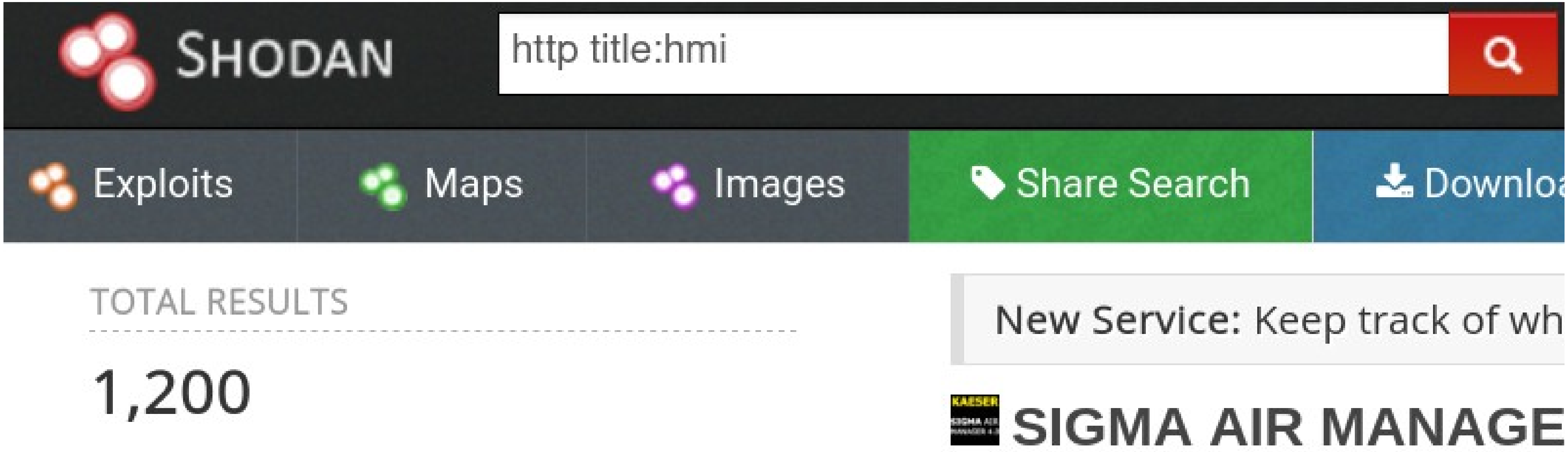
HMI Touch Screen

4G Router

Bivocom TG462 S
Touch Screen IoT Edge Gateway

Introduction

- HMI could be used as a pivot for adversaries
- In worse cases, HMIs are directly exposed to Internet



http title:hmi

TOTAL RESULTS

1,200

New Service: Keep track of wh

SIGMA AIR MANAGE

Emerging HMI Vendors

- Traditional manufacturers
  - Highly integrated into ecosystem, tested comprehensively (probably)
    - e.g. Import tag names directly from PLC
  - Built from the beginning
  - Software is considered as a product to sell

- Emerging manufacturers
  - Faster development cycle, using off-shelf hardware/software
  - Software is considered as a sales tool to sell hardware
    - Less costly, more friendly, bugs usually fixed rapidly

Security analysis *without* actual hardware

Goals & what we looked for

- Familiarization of modern HMI architecture
  - Embedded OS (e.g. WinCE6), non-100%-standard hardware
- Try to exploit it and see if modern HMIs are indeed secure by design

Security analysis *without* actual hardware

- We don’t want to purchase *every* hardware (practical concern)
  - Full firmware emulation (QEMU witchcraft)
  - Port software to other platform

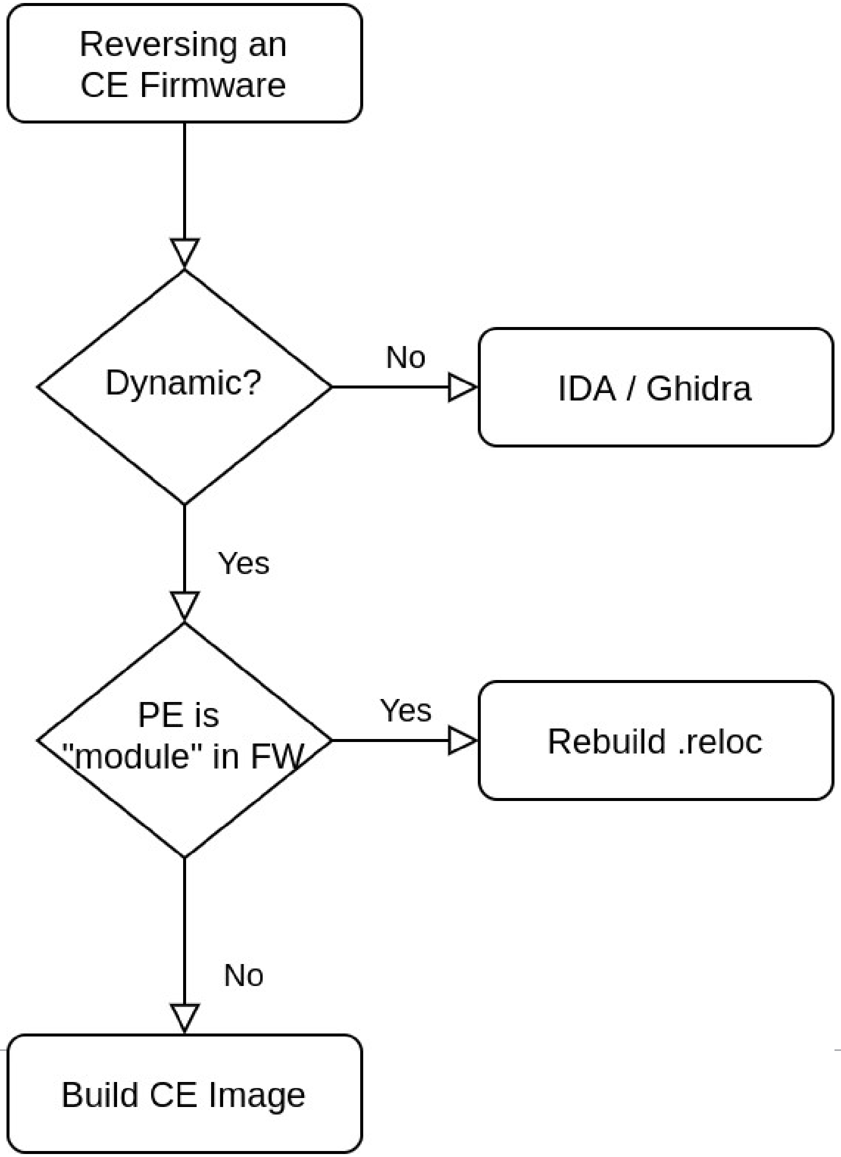
Firmware Files for Windows CE 6

- OS and bootloader are seperated files

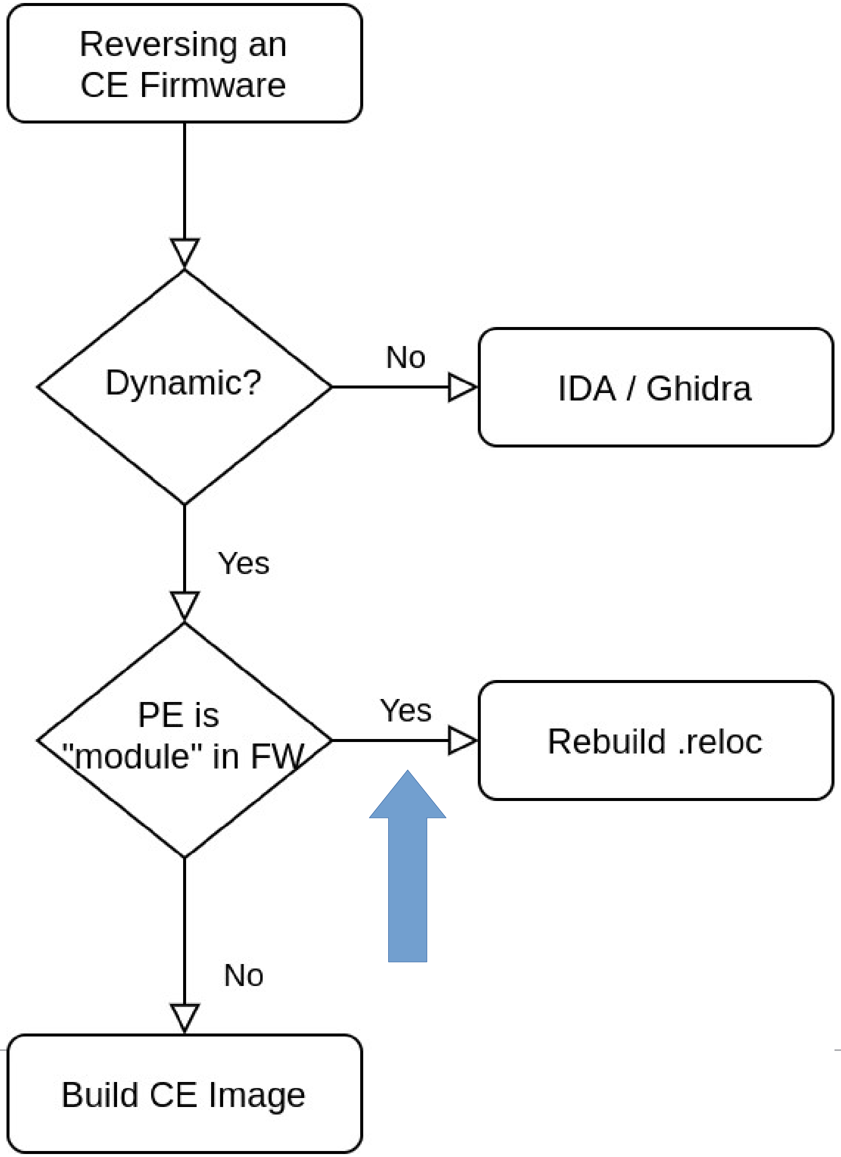
- Two types of firmware
  - .nb0 (1:1 mapping to flash memory)
  - .bin (organized, “B000FF bin format”)
    - https://forum.xda-developers.com/showthread.php?t=801167

- Contains “filesystem”
  - Modules (dlls, exes)
  - Files (others, but dlls/exes can be added as files too)

Main limitations for reverse engineering CE Firmware



Main limitations for reverse engineering CE Firmware



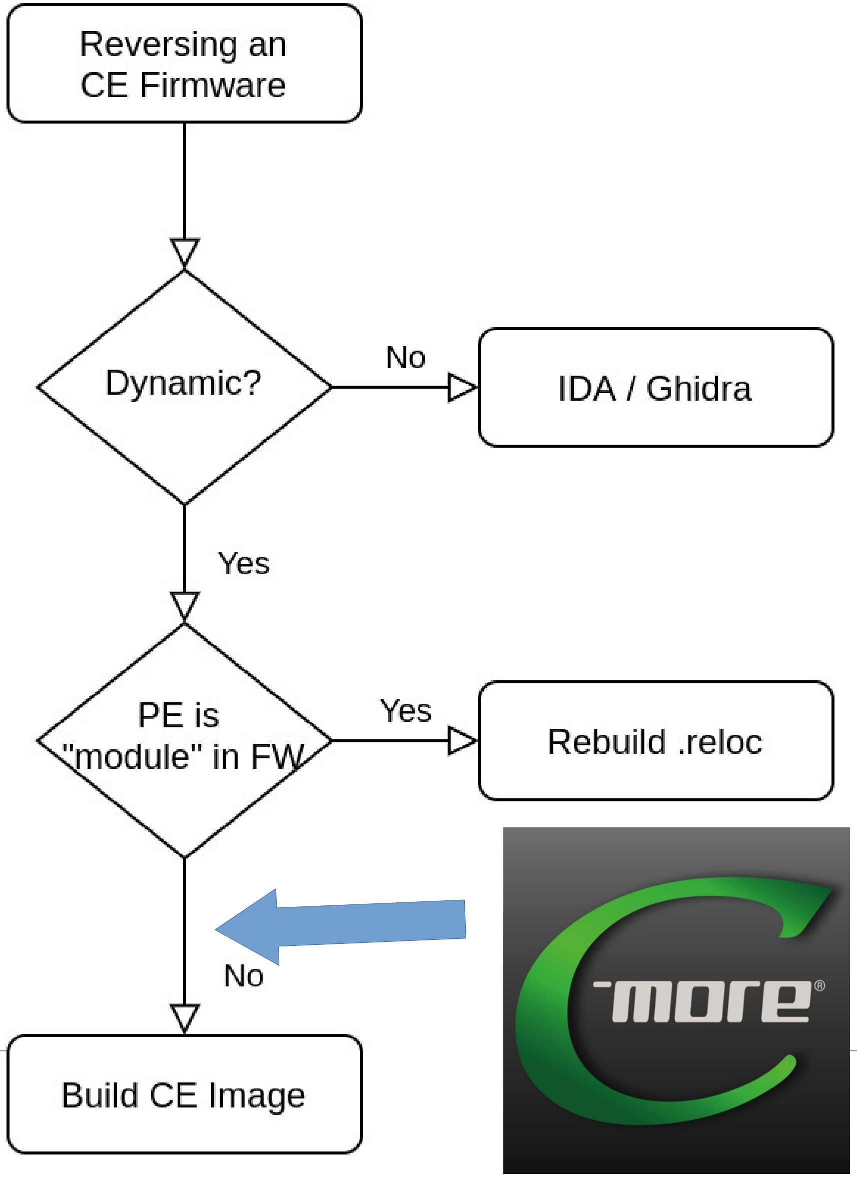
Main limitations for reverse engineering CE Firmware

- XIP (Execute-in-Place)
  - RAM is not required to hold the ROM's data as a program executes
  - Address is known at link time
    - MSVC Linker: `/IMAGEBASE`
    - Stripped of unnecessary sections (.reloc) to save space
  - ImageBase !== 0x10000000
  - Loading will NOT fail if ImageBase is occupied
    - Will load to arbitrary address, everything goes boom

Main limitations for reverse engineering CE Firmware

- XIP (Execute-in-Place)
  - Cannot move modules to other environment without major modification
    - We have solutions, will publish in future
  - Fortunately not the case for this firmware!

Main limitations for reverse engineering CE Firmware

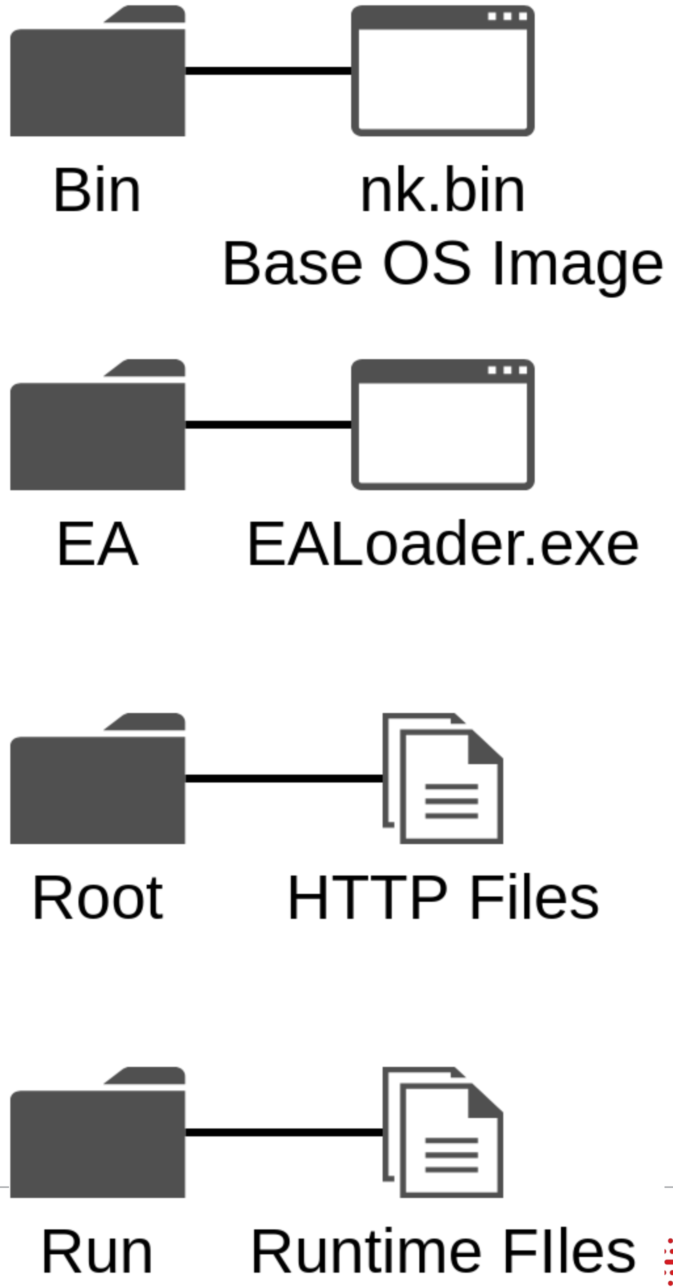


Our target platform

- C-more EA9 Series
  - Koyo Electronics (JTEKT Group)
- WinCE6 on ARMv4i
- i.MX51
  - Off-the-shelf hardware, smaller player
  - = Emerging vendor

C-More HMI update package

- Bundled with programming software
  - InstallShield
- .eas9 file
  - One Windows CE Image for base
  - Runtime files
    - Friendly debugging tools are included



C-More HMI update package

- Files are seperated by `([CZ]:\\\\.*?\\.[a-zA-Z]{3})`
  - Contains filename
- A trivial script to parse

Runtime porting

- Problems with porting
  - Usually we cannot use extracted PEs from NK.bin (XIP)
    - HMI runtime loader, etc
  - Missing DLLs
    - MFC, MS C Runtime Library…

Runtime porting

- Problems with porting
  - Usually we cannot use extracted PEs from NK.bin (XIP)
    - HMI runtime loader, etc
  - Missing DLLs
    - MFC, MS C Runtime Library…

- These are packed as “files” in C-more’s NK.bin
  - .reloc not stripped, ImageBase 0x10000
  - dumprom.exe to extract them
    - https://itsme.home.xs4all.nl/projects/xda/dumprom.html

Runtime porting

- Problems with porting
  - Emulator?
  - Target: ARMv4i / WinCE6

Runtime porting

- Problems with porting
  - Emulator?
  - Target: ARMv4i / WinCE6
    - We can use LOADCEPC (bootstrap with FreeDOS) on x86, but not ARM

Runtime porting

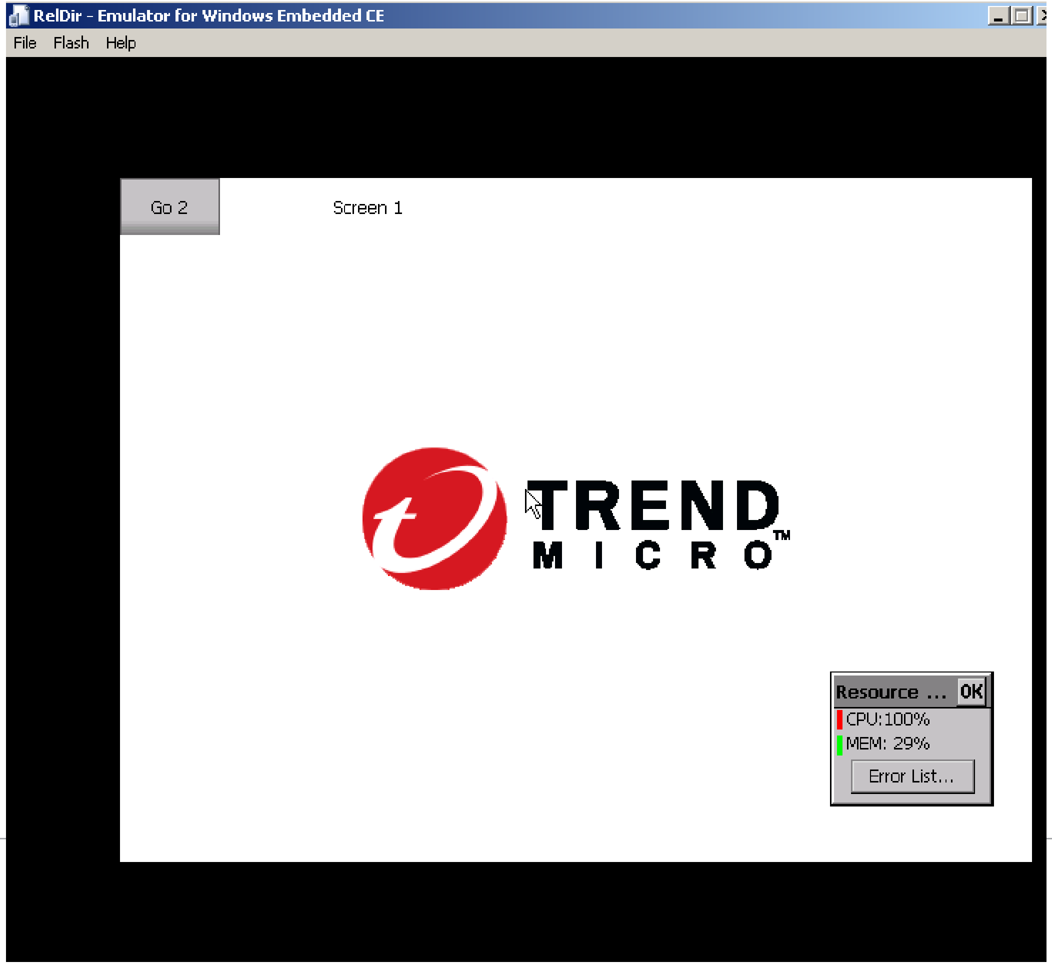
- Problems with porting
  - Emulator?
  - Target: ARMv4i / WinCE6
    - We can use LOADCEPC (bootstrap with FreeDOS) on x86, but not ARM
    - ARM CE emulator bundled with SDK from Microsoft

Runtime porting

- Problems with porting
  - Anyway…

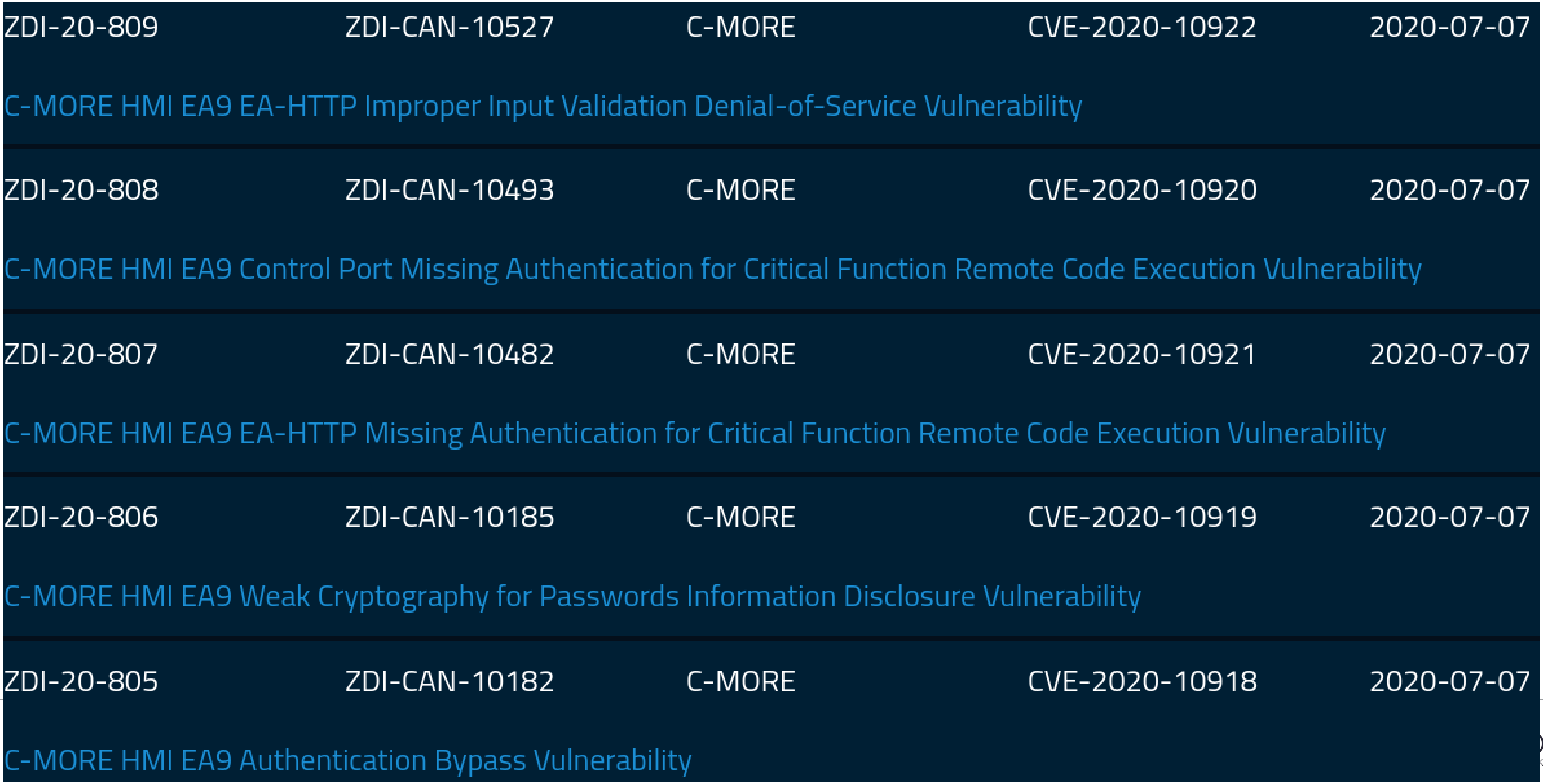
Runtime porting

- Problems with porting
  - Anyway…
  - Works emulated, but very slow



Results

Results



ZDI-20-809	ZDI-CAN-10527	C-MORE	CVE-2020-10922	2020-07-07
C-MORE HMI EA9 EA-HTTP Improper Input Validation Denial-of-Service Vulnerability				
ZDI-20-808	ZDI-CAN-10493	C-MORE	CVE-2020-10920	2020-07-07
C-MORE HMI EA9 Control Port Missing Authentication for Critical Function Remote Code Execution Vulnerability				
ZDI-20-807	ZDI-CAN-10482	C-MORE	CVE-2020-10921	2020-07-07
C-MORE HMI EA9 EA-HTTP Missing Authentication for Critical Function Remote Code Execution Vulnerability				
ZDI-20-806	ZDI-CAN-10185	C-MORE	CVE-2020-10919	2020-07-07
C-MORE HMI EA9 Weak Cryptography for Passwords Information Disclosure Vulnerability				
ZDI-20-805	ZDI-CAN-10182	C-MORE	CVE-2020-10918	2020-07-07
C-MORE HMI EA9 Authentication Bypass Vulnerability				

Results

- “Front door”
  - Authentication Bypass
  - Weak Cryptography for Passwords Information Disclosure
  - Control Port Missing Authentication for Critical Function Remote Code
- “Back door”
  - HTTP Missing Authentication for Critical Function Remote Code Execution
  - Improper Input Validation Denial-of-Service

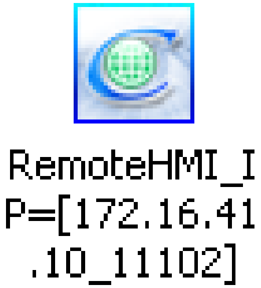
Front door

Authentication Bypass (CVE-2020-10918)

- Protocol does not implement state-machine correctly
- We can send “Post-Login” opcode without sending password
- Allows login & retrieval of screen content without credentials

Authentication Bypass (CVE-2020-10918)

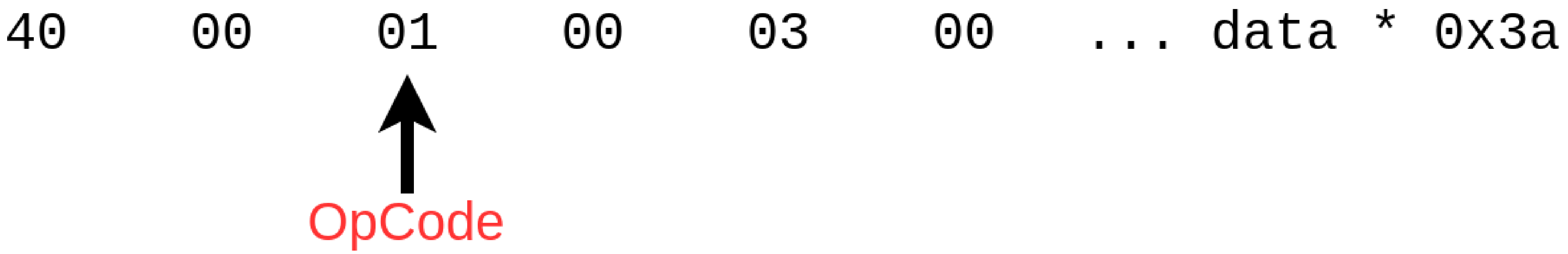
- C-more Remote Control Protocol (11102/tcp)
- VNC-like remote control capabilities
- Client can be downloaded from panel
  - Bizarrdly, gets IP and port from filename



RemoteHMI_IP=[172.16.41.10_11102]

Authentication Bypass (CVE-2020-10918)

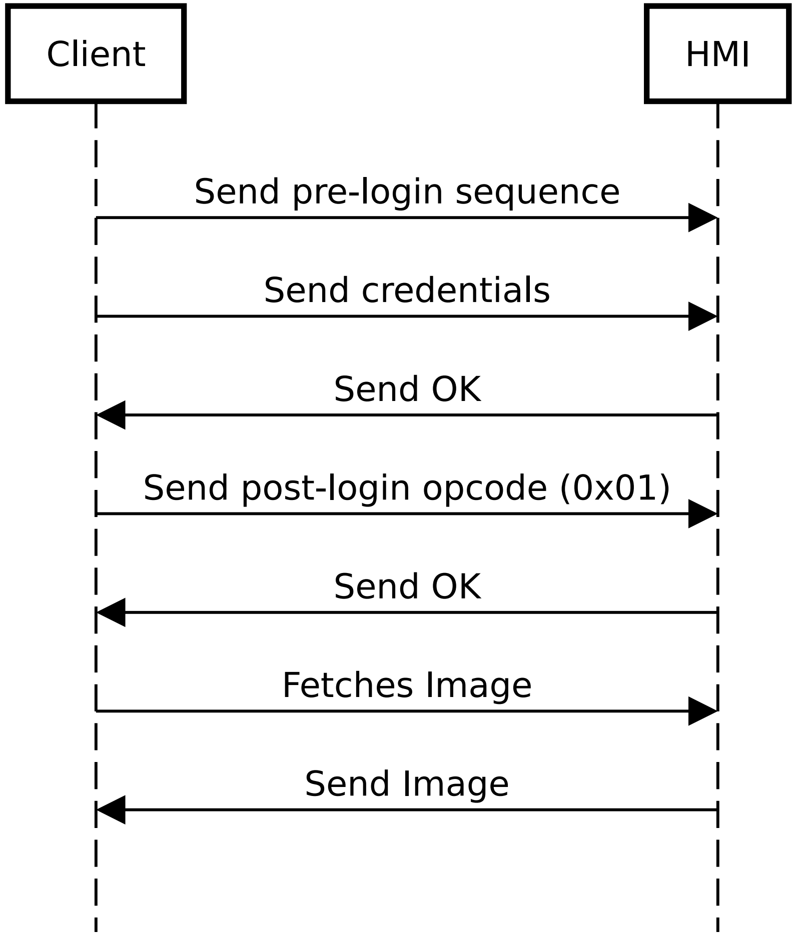
- C-more Remote Control Protocol (11102/tcp)
- Client → HMI Packet:



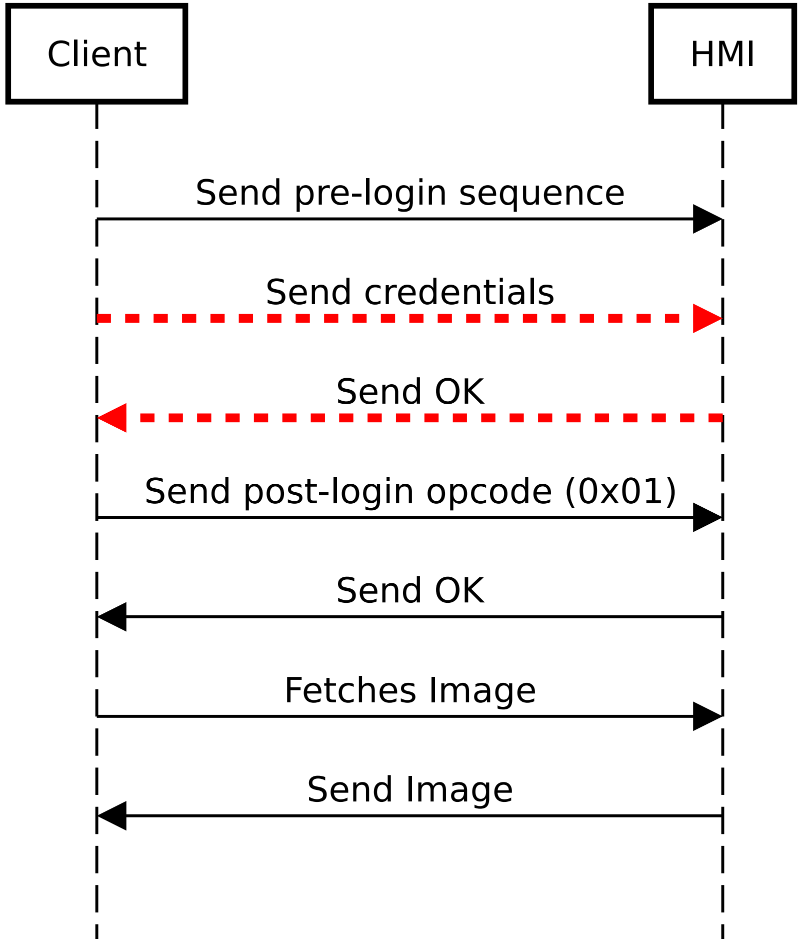
```
40    00    01    00    03    00    ... data * 0x3a
```

OpCode

Authentication Bypass (CVE-2020-10918)

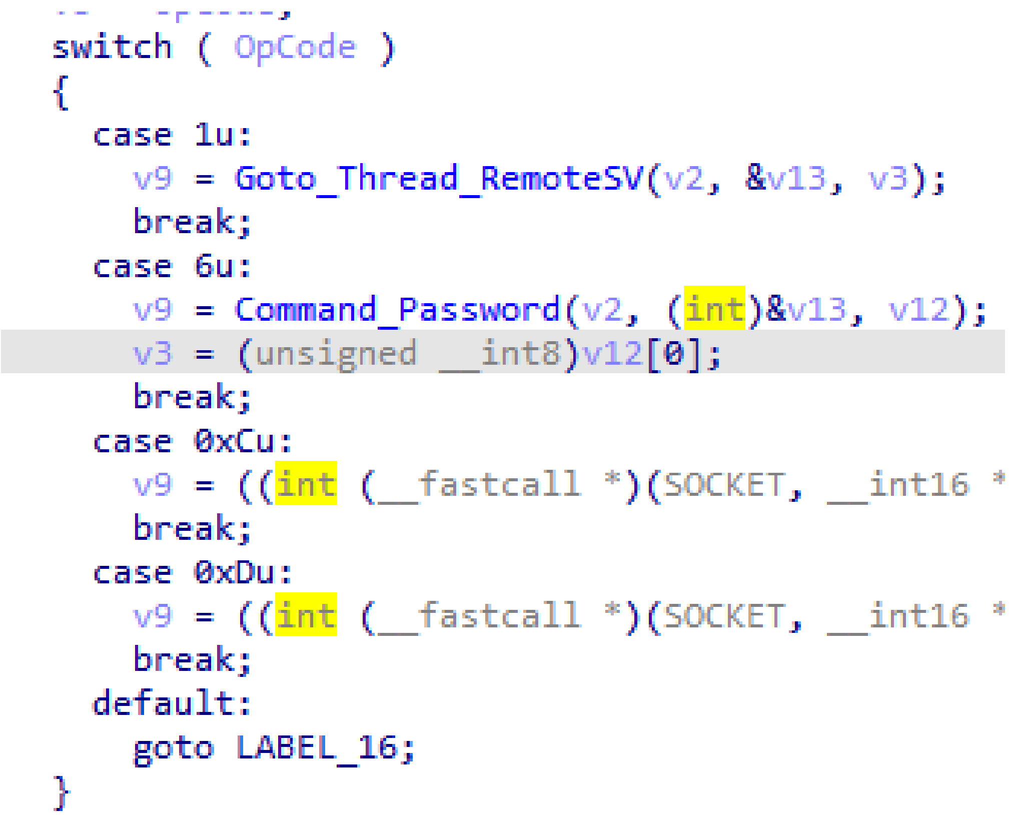


Authentication Bypass (CVE-2020-10918)



Authentication Bypass (CVE-2020-10918)

- State isn’t controlled properly…
- 0x06 goes to Command_Password and validates password
- 0x01 skips it



```
switch ( OpCode )
{
  case 1u:
    v9 = Goto_Thread_RemoteSV(v2, &v13, v3);
    break;
  case 6u:
    v9 = Command_Password(v2, (int)&v13, v12);
    v3 = (unsigned __int8)v12[0];
    break;
  case 0xCu:
    v9 = ((int (__fastcall *)(SOCKET, __int16 *
    break;
  case 0xDu:
    v9 = ((int (__fastcall *)(SOCKET, __int16 *
    break;
  default:
    goto LABEL_16;
}
```

Weak Cryptography for Passwords Information Disclosure (CVE-2020-10919)

- C-more Remote Control Protocol (11102/tcp)
- Sends password after opcode 0x06

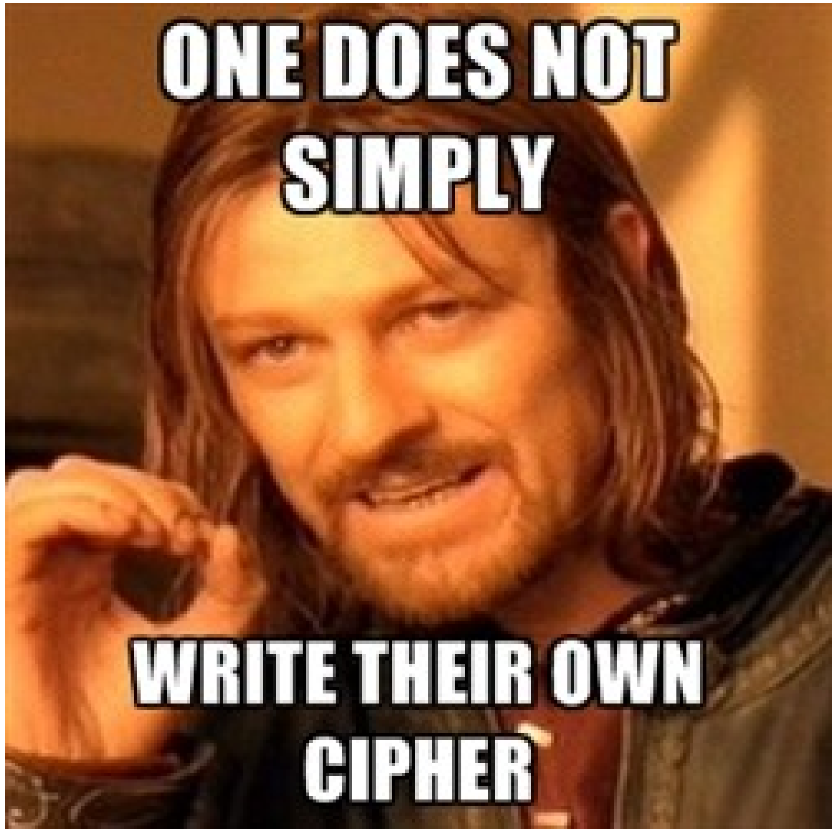
Username Ciphertext (128)	Username Key (128)
Password Ciphertext (128)	Password Key (128)

Weak Cryptography for Passwords Information Disclosure (CVE-2020-10919)

- Subtract same byte position in key to ciphertext for “decryption”
- Seems like a bug in software caused some zero-padding to be 0x01

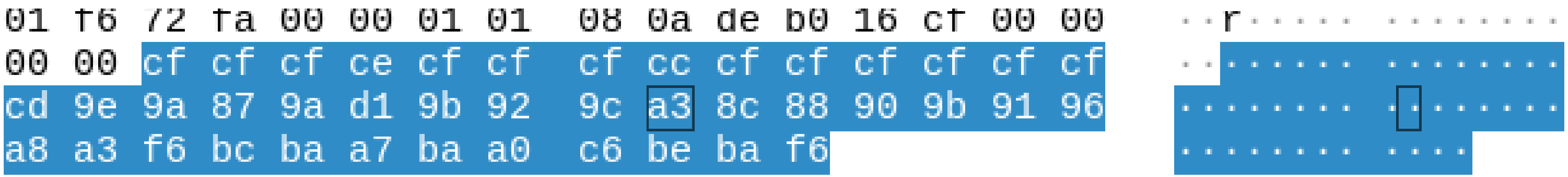
```
        5e    52    17    f1    72    fc    62    54    0a    55    ... key
 minus  5e    be    18    60    73    6e    62    b9    0a    c2    ... ciphertext
result  00    6c    01    6f    01    72    00    65    00    6d
               l           o           r           e           m
```

Weak Cryptography for Passwords Information Disclosure (CVE-2020-10919)



Control Port Missing Authentication for Critical Function Remote Code (CVE-2020-10920)

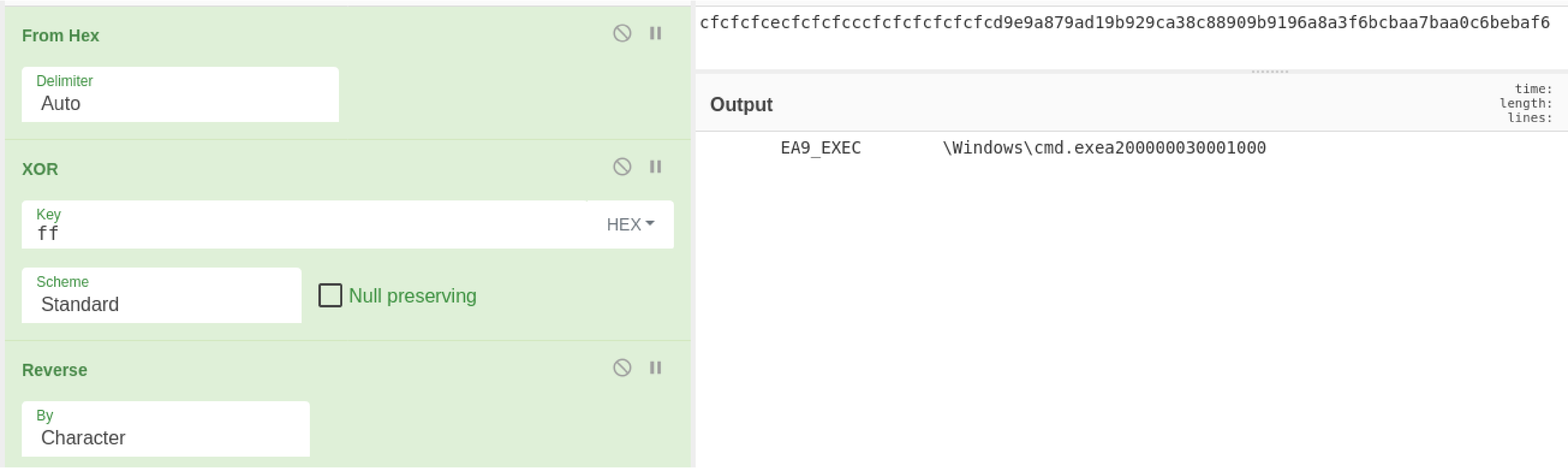
- C-more Project Control Protocol (9999/tcp)
  - Plaintext protocol?



```
01 f6 72 fa 00 00 01 01  08 0a de b0 16 cf 00 00   ..r..... ........
00 00 cf cf cf ce cf cf  cf cc cf cf cf cf cf cf   ........ ........
cd 9e 9a 87 9a d1 9b 92  9c a3 8c 88 90 9b 91 96   ........ ........
a8 a3 f6 bc ba a7 ba a0  c6 be ba f6               ........ ....
```

Control Port Missing Authentication for Critical Function Remote Code (CVE-2020-10920)

- C-more Project Control Protocol (9999/tcp)
  - Plaintext protocol!



From Hex

Delimiter: Auto

XOR

Key: ff HEX

Scheme: Standard

□ Null preserving

Reverse

By: Character

```
cfcfcfcecfcfcfcccfcfcfcfcfcfcd9e9a879ad19b929ca38c88909b9196a8a3f6bcbaa7baa0c6bebaf6
```

Output

```
time:
length:
lines:
```

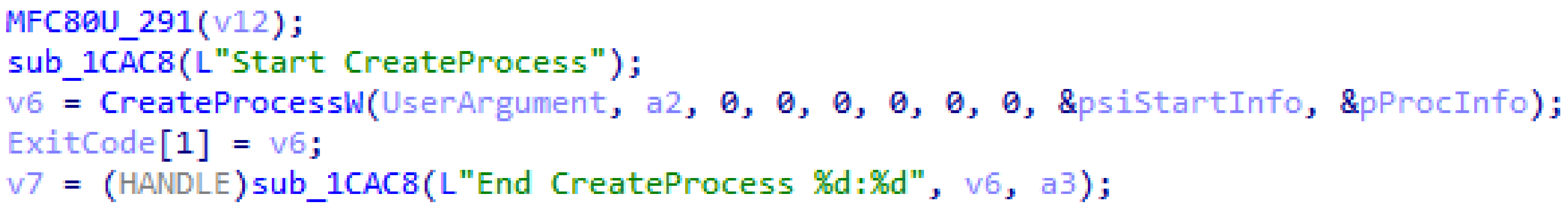
```
        EA9_EXEC         \Windows\cmd.exea200000030001000
```

Control Port Missing Authentication for Critical Function Remote Code (CVE-2020-10920)

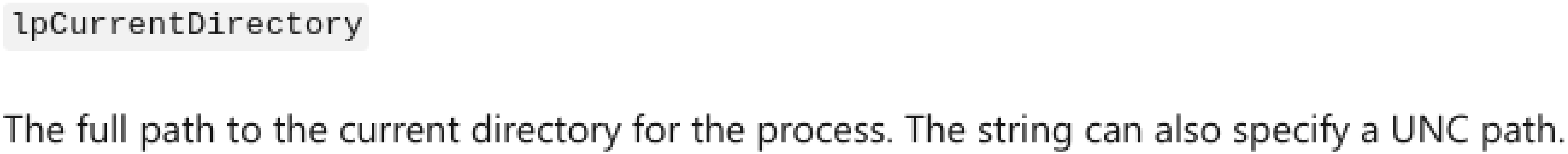
- Change screen
- Write files to panel
- Fetch files from panel
- Reboot
- Wipe panel!
- Execute arbitrary path (EA9_EXEC)

Control Port Missing Authentication for Critical Function Remote Code (CVE-2020-10920)

- Implementation of EA9_EXEC…
  - Argument is passed without sanitization to CreateProcessW
- No authorization required



```
MFC80U_291(v12);
sub_1CAC8(L"Start CreateProcess");
v6 = CreateProcessW(UserArgument, a2, 0, 0, 0, 0, 0, 0, &psiStartInfo, &pProcInfo);
ExitCode[1] = v6;
v7 = (HANDLE)sub_1CAC8(L"End CreateProcess %d:%d", v6, a3);
```

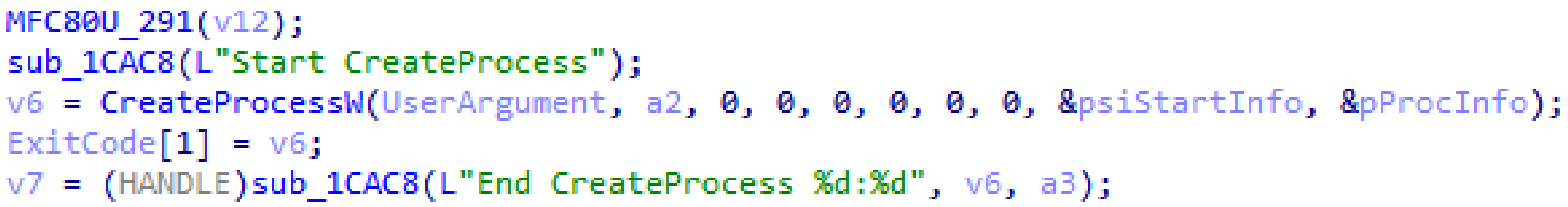


`lpCurrentDirectory`

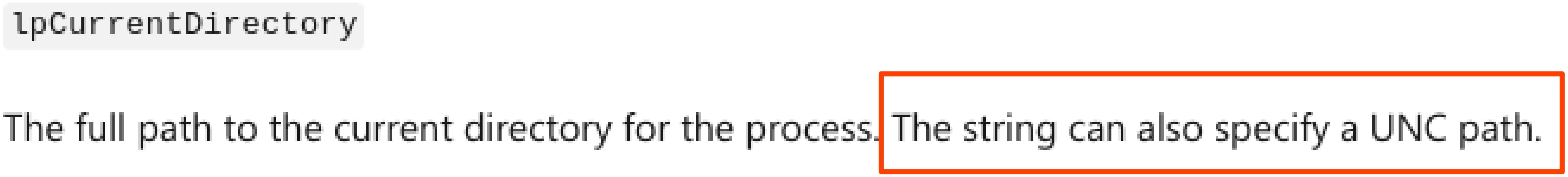
The full path to the current directory for the process. The string can also specify a UNC path.

Control Port Missing Authentication for Critical Function Remote Code (CVE-2020-10920)

- Implementation of EA9_EXEC…
  - Argument is passed without sanitization to CreateProcessW
- No authorization required



```
MFC80U_291(v12);
sub_1CAC8(L"Start CreateProcess");
v6 = CreateProcessW(UserArgument, a2, 0, 0, 0, 0, 0, 0, &psiStartInfo, &pProcInfo);
ExitCode[1] = v6;
v7 = (HANDLE)sub_1CAC8(L"End CreateProcess %d:%d", v6, a3);
```

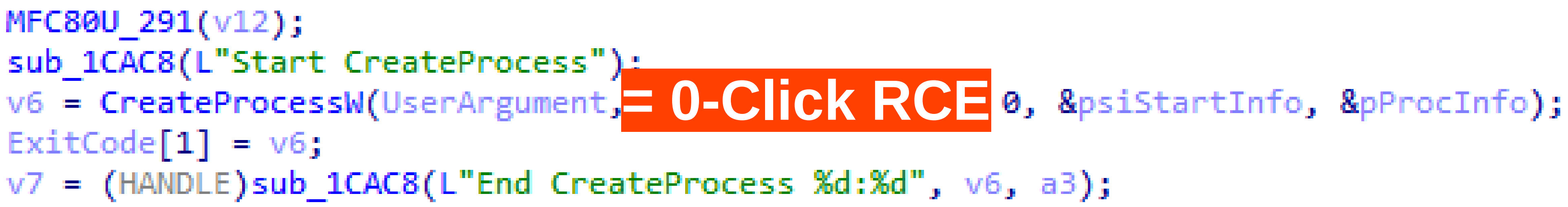


`lpCurrentDirectory`

The full path to the current directory for the process. The string can also specify a UNC path.

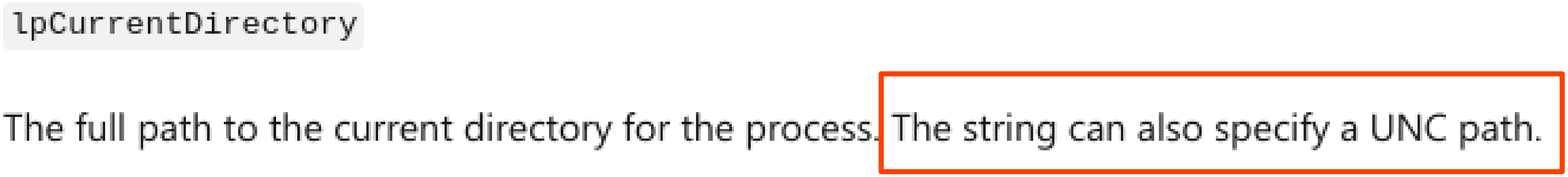
Control Port Missing Authentication for Critical Function Remote Code (CVE-2020-10920)

- Implementation of EA9_EXEC…
  - Argument is passed without sanitization to CreateProcessW
- No authorization required



```
MFC80U_291(v12);
sub_1CAC8(L"Start CreateProcess");
v6 = CreateProcessW(UserArgument,                 0, &psiStartInfo, &pProcInfo);
ExitCode[1] = v6;
v7 = (HANDLE)sub_1CAC8(L"End CreateProcess %d:%d", v6, a3);
```

= 0-Click RCE



`lpCurrentDirectory`

The full path to the current directory for the process. The string can also specify a UNC path.

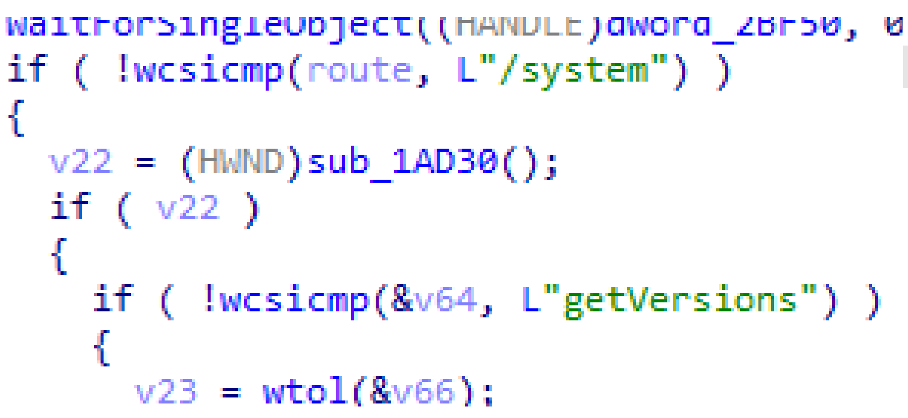
“Front Door” Demo

- https://powerbox-file.trend.org/SFDC/external_shared/97c439a67718be2a407ff64ef955972e.php

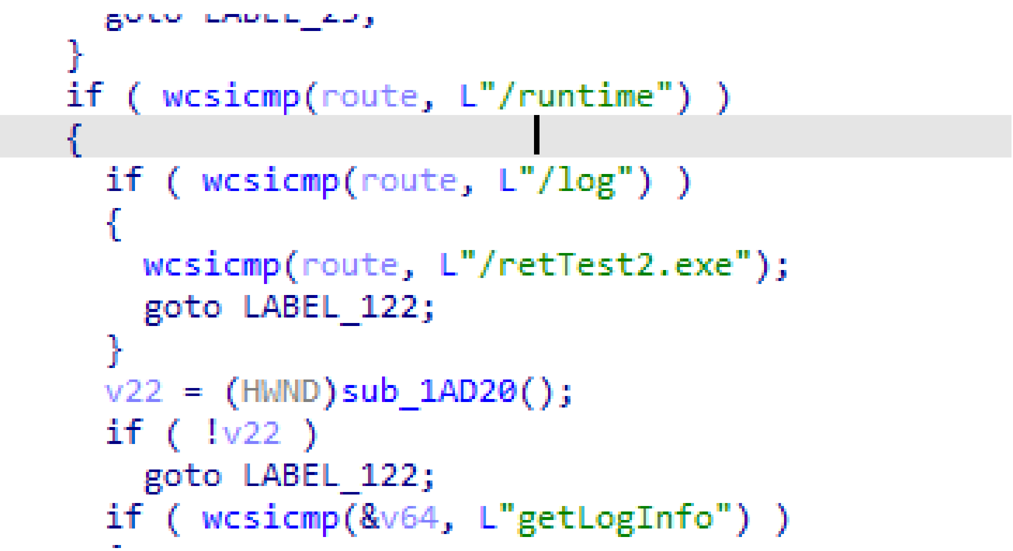
Back door

Back door

- Found something named very interesting in handler of EA-HTTP.exe!
  - 80/tcp, 443/tcp



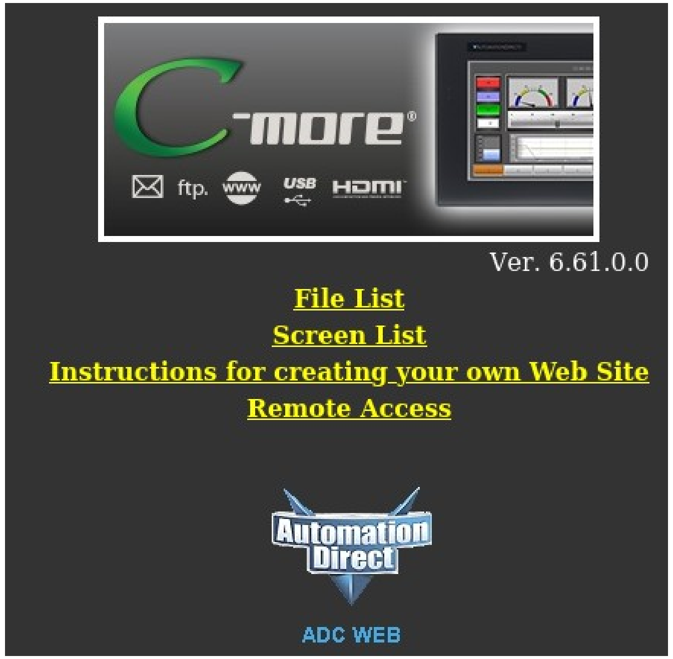
```
WaitForSingleObject((HANDLE)dword_2BF50, 0
if ( !wcsicmp(route, L"/system") )
{
  v22 = (HWND)sub_1AD30();
  if ( v22 )
  {
    if ( !wcsicmp(&v64, L"getVersions") )
    {
      v23 = wtol(&v66);
```



```
  goto LABEL_23;
}
if ( wcsicmp(route, L"/runtime") )
{
  if ( wcsicmp(route, L"/log") )
  {
    wcsicmp(route, L"/retTest2.exe");
    goto LABEL_122;
  }
  v22 = (HWND)sub_1AD20();
  if ( !v22 )
    goto LABEL_122;
  if ( wcsicmp(&v64, L"getLogInfo") )
```

Missing Authentication for Critical Function Remote Code Execution (CVE-2020-10921)

- EA-HTTP.exe
  - Serve both static file and some API endpoints
- Some undocumented APIs?



Ver. 6.61.0.0

File List

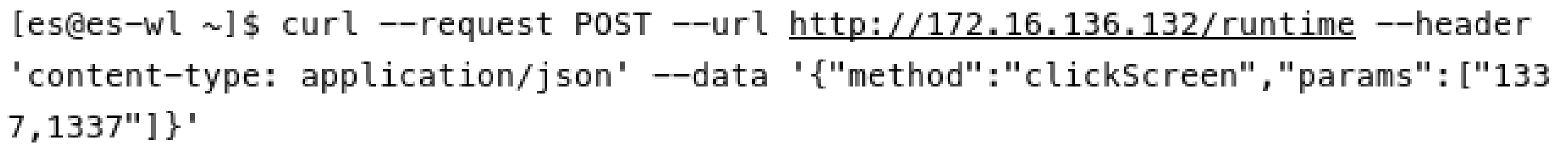
Screen List

Instructions for creating your own Web Site

Remote Access

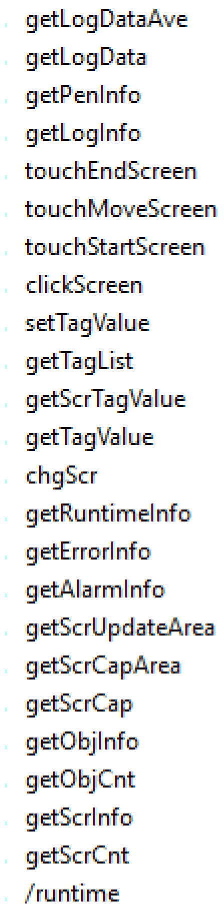
Missing Authentication for Critical Function Remote Code Execution (CVE-2020-10921)

- Get panel info, take screenshot, change system time…
- Click on screen!

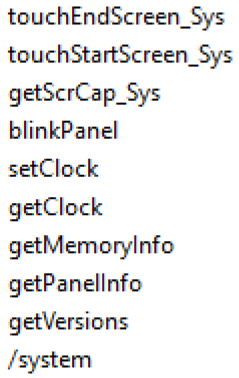


```
[es@es-wl ~]$ curl --request POST --url http://172.16.136.132/runtime --header
'content-type: application/json' --data '{"method":"clickScreen","params":["133
7,1337"]}'
```

- Authorization not required at all



getLogDataAve
getLogData
getPenInfo
getLogInfo
touchEndScreen
touchMoveScreen
touchStartScreen
clickScreen
setTagValue
getTagList
getScrTagValue
getTagValue
chgScr
getRuntimeInfo
getErrorInfo
getAlarmInfo
getScrUpdateArea
getScrCapArea
getScrCap
getObjInfo
getObjCnt
getScrInfo
getScrCnt
/runtime



touchEndScreen_Sys
touchStartScreen_Sys
getScrCap_Sys
blinkPanel
setClock
getClock
getMemoryInfo
getPanelInfo
getVersions
/system

Improper Input Validation Denial-of-Service (CVE-2020-10922)

- Simply send a malformed (e.g. wrong JSON type) to DoS
- Would crash EA-HTTP and prevent further requests
- Does not impact critical panel functions

Conclusion

- “Secure by design” must be included for any project
- Network Segmentation might save you from vulnerable devices
- Obscurity is not security

Future Work

- More vulnerabilities
- Static reconstruction of relocation information to re-bundle XIP files
  - Will publish in future!

Thank you!

talun_yen at trendmicro dot com
@evanslify