



GHOSTS IN THE MACHINE

FIRMWARE VULNERABILITIES IN CRITICAL INFRASTRUCTURE

/WHOIS NATE WARFIELD

- Director of Research @ Eclypsium
- F5 Networks, Microsoft (MSRC, M365)
- Destroyer of network devices
- 4th time BruCON speaker
- Security researcher
- Socials: @n0x08

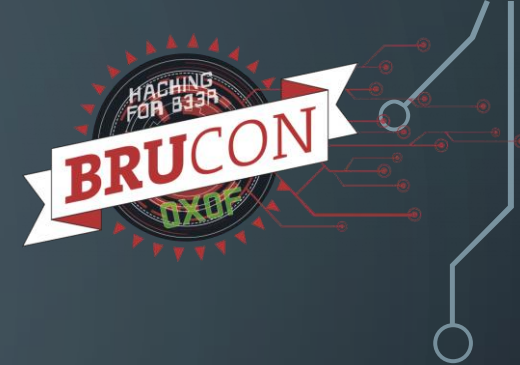


AGENDA & MOTIVATIONS

- Current firmware landscape
- Firmware analysis 101
- Open-source toolsets
- Obligatory ChatGPT references
- Wanna see a dead body?
- Conclusions
- I've done defensive talks
- I've done offensive talks
- This is an educational talk
- Firmware security needs humans
- BruCON attracts up & coming people
- B33R

WHY SHOULD WE CARE?





FIRMWARE IS SO ~~HOT~~ HACKED RIGHT NOW

- Jan 30: Second set of BMC vulns disclosed
- March 1: Black Lotus disclosed
- March 16: Fortinet attacks by UNC3886
- April 7: MSI breach & stolen source code announced
- May 31: Gigabyte backdoor disclosed
- June 1: Barracuda announces 0-day attacks
- June 13: Binding Operational Directive 23-02
- June 14: Harden BMCs
- July 25: Citrix 0-day announced
- Sept 8: Mandiant details Barracuda backdoors



National Security Agency

Cybersecurity and Infrastructure Security Agency

Cybersecurity Information

TLP: CLEAR

Harden Baseboard Management Controllers

Summary

Baseboard management controllers (BMCs) are trusted components designed into a computer's hardware that operate separately from the operating system and firmware to allow for remote management and control, even when the system is shut down. This Cybersecurity Information Sheet (CSI), authored by the National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA), highlights threats to BMCs and details actions organizations can use to harden them. NSA and CISA encourage all organizations managing relevant servers to apply the recommended actions in this CSI.

Malicious actors target overlooked firmware

BINDING OPERATIONAL DIRECTIVES

Binding Operational Directive 23-02

June 13, 2023

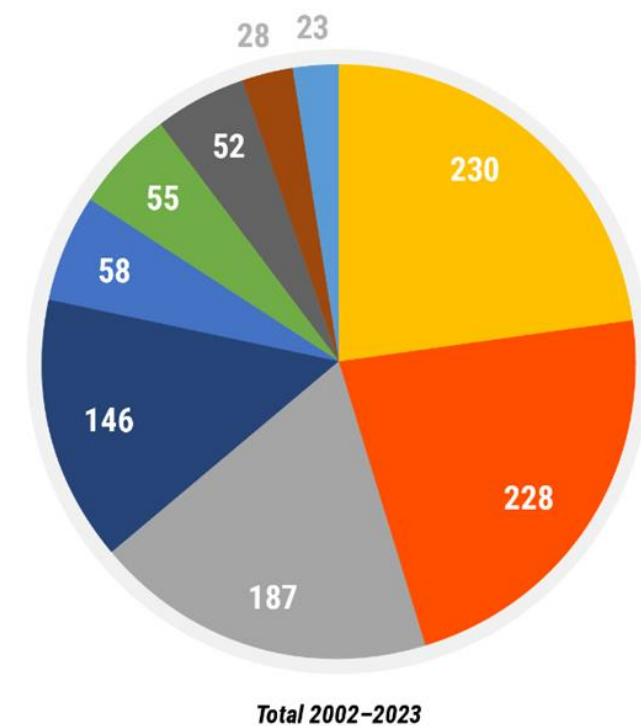
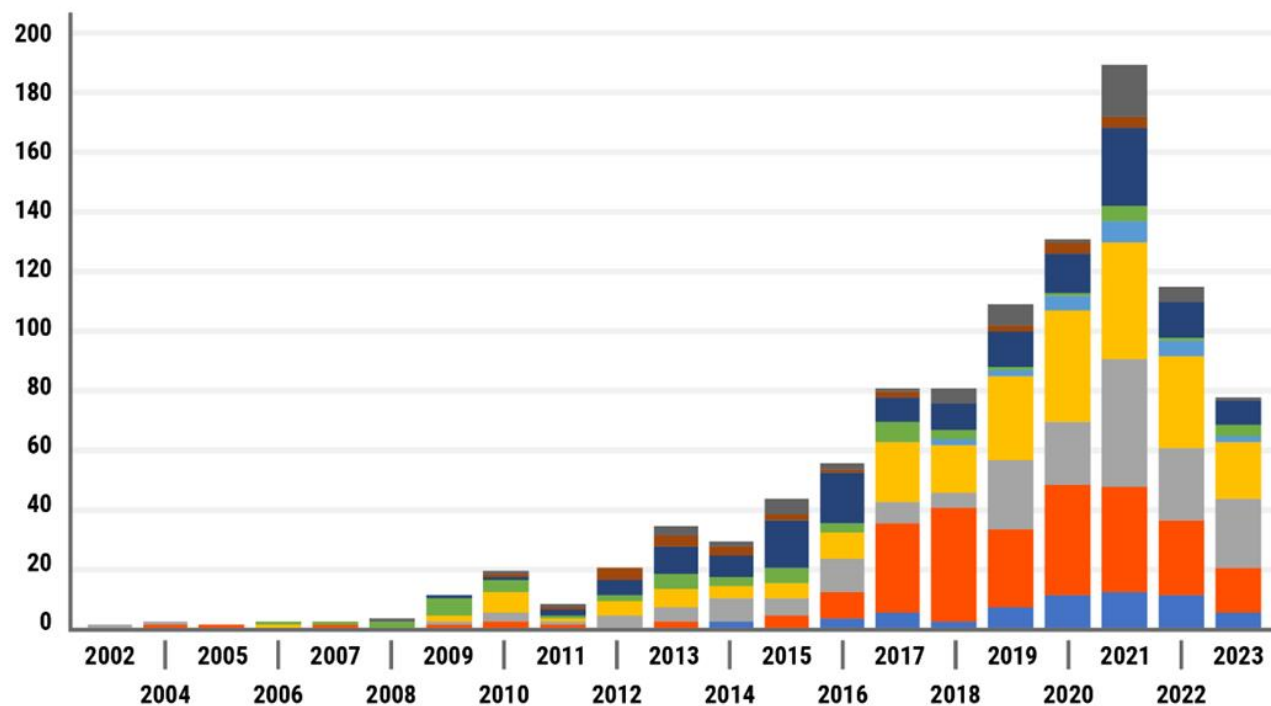
RELATED TOPICS: [CYBERSECURITY BEST PRACTICES](#)



MITIGATING THE RISK FROM INTERNET-EXPOSED MANAGEMENT INTERFACES

This page contains a web-friendly version of the Cybersecurity and Infrastructure Security Agency's Binding Operational Directive 23-02: Mitigating the Risk from Internet-Exposed Management Interfaces.

KNOWN EXPLOITED VULNERABILITIES



FIRMWARE ANALYSIS

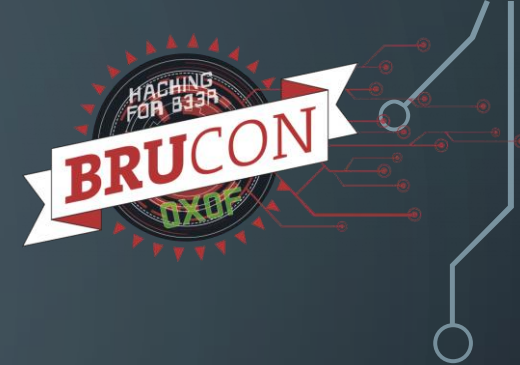
“Firmware is the immutable law that governs the machine, the commandments etched into its very being”

--ChatGPT



COMMERCIAL OFFERINGS

- Microsoft Defender for IoT
- OneKey
- Finite State
- Netrise
- Nozomi Networks
- Bugprove
- Limited firmware support
- SBOM
- Identify CVEs
- Identify CWEs
- Crypto material/passwords
- You're paying for the GUI



INITIAL ANALYSIS & UNPACKING

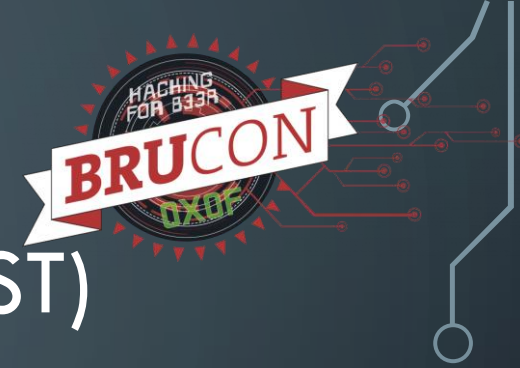
- Firmware requires unpacking first
- Complexity varies by vendor and version
- Sometimes binwalk is enough
- Somethings literally nothing will work
- Unblob >> binwalk
- Custom packing is a thing
- 7zip is your friend

C:\Users\mate.warfield_eclyps\Downloads\build-13.1-9.60_nc_64.tgz\build_artesa_9_60_nc_64.tar\nc-13.1-9.60.gz\kernel.nc.a

Name	Size	Virtual Size	Offset	Virtual Address	Type
mfs	549 453 824	549 453 824	24 790 160	0xFFFFFFFF81B...	PROGBITS
.text	14 351 512	14 351 512	868 352	0xFFFFFFFF802...	PROGBITS
.data	6 254 473	6 254 473	18 530 304	0xFFFFFFFF815...	PROGBITS
.rodata	3 199 372	3 199 372	15 220 736	0xFFFFFFFF810...	PROGBITS
.symtab	1 075 200	1 075 200	574 373 776	0x0	SYMTAB
.strtab	1 039 999	1 039 999	575 448 976	0x0	STRTAB
.SUNW_ctf	936 471	936 471	576 488 976	0x0	PROGBITS
.dynsym	417 960	417 960	135 728	0xFFFFFFFF802...	DYNSYM
.dynstr	314 487	314 487	553 688	0xFFFFFFFF802...	STRTAB
.hash	135 312	135 312	416	0xFFFFFFFF802...	HASH

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	XML document, version: "1.0"
144	0x90	Copyright string: "Copyright>Copyright 2007-2021, Raritan Americas, Inc.</Copyright>"
154	0x9A	Copyright string: "Copyright 2007-2021, Raritan Americas, Inc.</Copyright>"
199	0xC7	Copyright string: "Copyright>"
18746948	0x11E0E44	MySQL MISAM index file Version 7

DECIMAL	HEXADECIMAL	DESCRIPTION
320	0x140	Squashfs filesystem, little endian, version 4.0, compression:xz, size: 9873159 bytes, 1164 inodes, blocksize: 131072 bytes, created: 2022-10-16 22:25:56
9876840	0x96B568	uImage header, header size: 64 bytes, header CRC: 0x438AF872, created: 2022-10-16 20:29:00, image size: 2588552 bytes, Data Address: 0x20008000, Entry Point: 0x20008000, data CRC: 0x2F031CA1, OS: Linux, CPU: ARM, image type: OS Kernel Image, compression type: none, image name: "Linux-5.10.136-sam9"



STATIC APPLICATION SECURITY TESTING (SAST)

- Static analysis requires source code
- D(ynamic)AST analyzes running applications
- DAST is out of scope for this talk
- Semgrep (multi-language, has paid version)
- Progpilot (PHP)
- OSS tools are very limited (big money in SAST)

```
<?php
require_once('config/config.php');
require_once('include/utils.php');
require_once('include/class.sdk.php');

$SdkAdminObj = new SdkAdminClass();

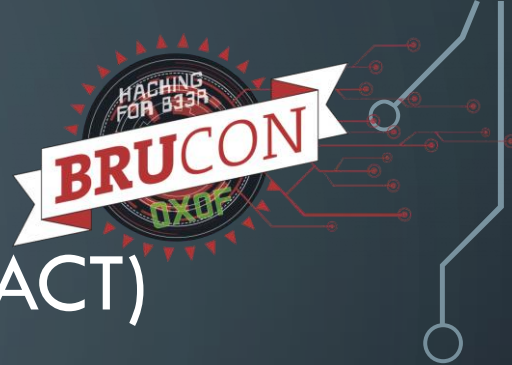
if (isset($_POST['stopRunningJobId'])){
    $id = $_POST['stopRunningJobId'];
    $filename = "/mnt/sdk/tmp/job-$id.pid";
    if (file_exists($filename)){
        $file = fopen($filename,"r");
        if ($file !== FALSE) {
            $pid = fread($file,filesize($filename));
            fclose($file);
            exec(escapeshellcmd("kill -15 " . escapeshellarg($pid)))

            for ($i=0; $i< $i++) {
                sleep(1);
                if (!file_exists("/proc/$pid")) break;
            }
            if (file_exists("/proc/$pid")) {
                exec(escapeshellcmd("kill -9 " . escapeshellarg($pid)))
                sleep(1);
            }
            unlink($filename);
            syslog(LOG_WARNING, "sdk: killing job $id (pid $pid)");
        }
    }
}
```

AUTOMATE ALL THE THINGS

- Firmware analysis is generally slow
- Hard to perform analysis at scale
- Expensive to buy hardware
 - Wanna loan me your datacenter?
- EOL devices are still prevalent
- I'm not an RE expert & have limited time



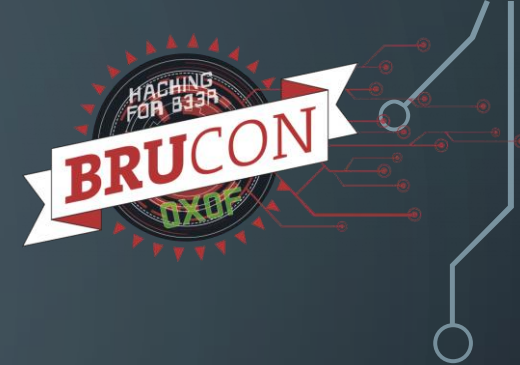


FIRMWARE ANALYSIS AND COMPARISON TOOL (FACT)

- Automated unpacking via binwalk
- Password cracking via john the ripper
- Vulnerability identification
- QEMU emulation
- Database backend
- Web interface
- Fast(ish) with powerful VM

<input checked="" type="checkbox"/> binwalk	<input type="checkbox"/> input vectors
<input checked="" type="checkbox"/> cpu architecture	<input checked="" type="checkbox"/> interesting uris
<input type="checkbox"/> crypto hints	<input checked="" type="checkbox"/> ip and uri finder
<input checked="" type="checkbox"/> crypto material	<input type="checkbox"/> ipc analyzer
<input checked="" type="checkbox"/> cve lookup	<input checked="" type="checkbox"/> kernel config
<input type="checkbox"/> cwe checker	<input checked="" type="checkbox"/> known vulnerabilities
<input type="checkbox"/> device tree	<input type="checkbox"/> printable strings
<input type="checkbox"/> elf analysis	<input type="checkbox"/> qemu exec
<input checked="" type="checkbox"/> exploit mitigations	<input checked="" type="checkbox"/> software components
<input type="checkbox"/> file system metadata	<input type="checkbox"/> source code analysis
<input type="checkbox"/> hardware analysis	<input type="checkbox"/> string evaluator
<input type="checkbox"/> hashlookup	<input type="checkbox"/> tlsh
<input type="checkbox"/> information leaks	<input checked="" type="checkbox"/> users and passwords
<input checked="" type="checkbox"/> init systems	

Latest Firmware Submissions		
Hikvision DS-2CD4112FWD-IZ - 1 (camera)	2023-09-01 21:49:28	None
Robustel R3000 - 5.1.0 (industrial router)	2023-04-19 22:28:40	generic_carver
Racom Midge2 - 4.6.40.102 (industrial router)	2023-04-18 17:49:58	generic_carver
Racom Midge2 - 4.6.40.103 (industrial router)	2023-04-18 15:52:55	generic_carver
Supermicro X13SEM-F - x13sem-f-bmc-web (BMC)	2023-04-07 16:12:24	generic_carver
Supermicro X13SEM-F - X13SEM-F (BMC)	2023-04-07 04:35:01	generic_carver
Supermicro X13DDW-A - X13DDW-A (BMC)	2023-04-07 04:33:46	generic_carver
Citrix ADC - 13.1-42.47 (BIOS)	2023-04-06 17:39:22	UEFI
Citrix ADC - 13.1-42.47 (9_16k BMC) (BMC)	2023-04-06 17:21:17	7z
Citrix ADC - 13.1-42.47 (BMC)	2023-04-05 22:59:46	generic_carver



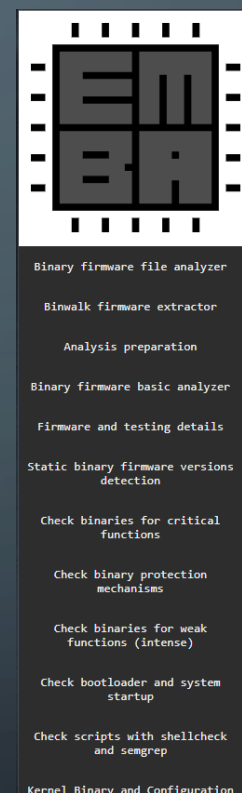
EMBEDDED ANALYZER (EMBA)

- CLI; web reports only
- Known Exploited Vulnerability correlation
- Generates SBOM (CycloneDX)
- Exploit data; availability, capabilities
- Uses semgrep for SAST
- ChatGPT integration (experimental)

```
root:ToC0v8qxP13qs:0:0:root:/root:/bin/sh
admin:yiVXjXdLpGfug:0:0:admin:/bin/sh
root:yiNNyNaXWRwx.:0:0:root:/root:/bin/sh

Loaded 3 password hashes with 2 different salts (1.5x same-salt boost)
12345          (admin)
duhao         (root)

[*] John the ripper final status: 2 password hashes cracked, 1 left
[*] Password hash cracked: admin:12345:0:0:admin:/bin/sh
[*] Password hash cracked: root:duhao:0:0:root:/root:/bin/sh
```



```
[*] Final aggregator

[+] Tested firmware: /home/nate/digicap_V5.2.0_build_181123.dav
[+] EMBA start command: ./emba.sh -c -f /home/nate/digicap_V5.2.0_build_181123.dav -l
[+] Detected architecture and endianness (verified): ARM / EL
[+] Operating system detected (verified): Linux / v3.0.8

[+] 141 files and 40 directories detected.
[+] Found 1 issues in 1 shell scripts.
[+] Found 243 yara rule matches in 141 files.
[+] Found 3 successful emulated processes (user mode emulation).

[+] Found the following configuration issues:
Found 109 areas with weak permissions.
Found 1 authentication issues.
Found 12 password related details via STACS (2 passwords cracked.)
Found 7 kernel modules with 1 licensing issues.
Found 73 security related kernel settings for review.
Found 0 interesting files and 1 files that could be useful for post-exploitation.

[+] Found 33 (79%) binaries without enabled stack canaries in 42 binaries.
[+] Found 41 (98%) binaries without enabled RELRO in 42 binaries.
[+] Found 7 (17%) binaries without enabled NX in 42 binaries.
[+] Found 21 (50%) binaries without enabled PIE in 42 binaries.
[+] Found 31 (74%) stripped binaries without symbols in 42 binaries.

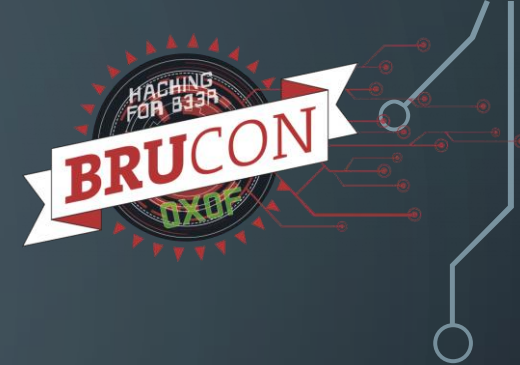
[+] cwe-checker found a total of 3226 of the following security issues:
CWE119 - Buffer Overflow - 1 times.
CWE125 - Out-of-bounds Read - 4 times.
CWE134 - Externally Controlled Format String - 181 times.
CWE190 - Integer Overflow or Wraparound - 23 times.
CWE215 - Information Exposure Through Debug Information - 3 times.
CWE415 - Double Free - 2 times.
CWE416 - Use After Free - 12 times.
CWE467 - Use of sizeof on a Pointer Type - 72 times.
CWE476 - NULL Pointer Dereference - 511 times.
CWE676 - Use of Potentially Dangerous Function - 2164 times.
CWE782 - Exposed IOCTL with Insufficient Access Control - 232 times.
CWE787 - Out-of-bounds Write - 14 times.
CWE789 - Large memory allocation - 7 times.
```

```
[+] Warning: Possible authorized_key backdoor detected: /logs/firmware/unblob_extracted/firmware_extract/5111808-9764864.jffs2_new_extract/user_home/keymgmt/.ssh/authorized_keys
logs/firmware/unblob_extracted/firmware_extract/5111808-9764864.jffs2_new_extract/user_home/mgmt/.ssh/authorized_keys (-rw-r--r-- root root)
[+] Warning: Possible authorized_key backdoor detected: /logs/firmware/unblob_extracted/firmware_extract/5111808-9764864.jffs2_new_extract/user_home/mgmt/.ssh/authorized_keys
logs/firmware/unblob_extracted/firmware_extract/5111808-9764864.jffs2_new_extract/user_home/solusr/.ssh/authorized_keys (-rw-r--r-- root root)
[+] Warning: Possible authorized_key backdoor detected: /logs/firmware/unblob_extracted/firmware_extract/5111808-9764864.jffs2_new_extract/user_home/solusr/.ssh/authorized_keys
/etc/defconfig/user_home/keymgmt/.ssh/authorized_keys (-rw-r--r-- root root)
```


TUNING EMBA

- 76 modules; 44 test modules, 17 prep modules
- 2-36hrs per analysis (!)
- `emba/config/module_blacklist.txt`
 - `S99_grepit`
 - `S110_yara_check`
 - `S15_radare_decompile_checks`
- Test with a defined set of modules
- `emba/helpers/running_modules.sh`
- Add more resources
 - I run 12x 3.8Ghz AMD Ryzen cores + 32GB RAM





CHATGPT ALL SOME OF THE THINGS

This code is a sequence of x86 assembly instructions that initialize values in memory. The `mov` instruction copies a value into a memory location. The memory locations being referenced are relative to the base pointer `rbp`. The values being copied into these locations appear to be ASCII codes for characters, indicated by the use of hexadecimal values (e.g. `20h` is the ASCII code for the character `' '`). The resulting string of characters might represent a message or data of some sort.

NW print the string of characters

The string of characters can be constructed from the ASCII codes in the code:

```
diff
-k
zfguijkophju@*%1]
```

```
lea rdx, [rbp+var_A0]
lea rax, [rbp+var_90]
mov rsi, rdx
mov rdi, rax
call fwdec
lea rsi, [rbp+var_E0]
lea rcx, [rbp+var_A0]
lea rax, [rbp+var_80]
lea rdx, [rbp+var_B0]
mov [rsp+210h+var_210], rdx
mov r9, rsi
mov r8, rcx
mov rcx, rax
mov edx, offset aSSSSDevNull21_0 ; "%s %s/%s %s >/dev/null 2>&1"
mov esi, 3FFh ; maxlen
mov edi, offset buf ; s
mov eax, 0
call _sprintf
mov edi, offset buf
call executecmd
test eax, eax
jz loc_401AE1
```

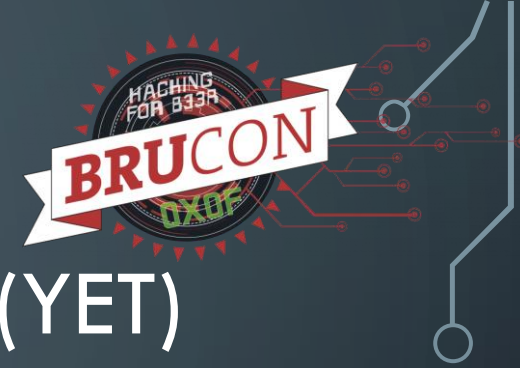
```
mov [rbp+var_9F], 0
mov [rbp+var_C0], 20h ; ' '
mov [rbp+var_BF], 68h ; 'k'
mov [rbp+var_BE], 0
mov [rbp+var_E0], 7Ah ; 'z'
mov [rbp+var_DF], 66h ; 'f'
mov [rbp+var_DE], 67h ; 'g'
mov [rbp+var_DD], 75h ; 'u'
mov [rbp+var_DC], 69h ; 'i'
mov [rbp+var_DB], 6Ah ; 'j'
mov [rbp+var_DA], 68h ; 'k'
mov [rbp+var_D9], 6Fh ; 'o'
mov [rbp+var_D8], 70h ; 'p'
mov [rbp+var_D7], 68h ; 'h'
mov [rbp+var_D6], 6Ah ; 'j'
mov [rbp+var_D5], 75h ; 'u'
mov [rbp+var_D4], 40h ; '@'
mov [rbp+var_D3], 2Ah ; '*'
mov [rbp+var_D2], 25h ; '%'
mov [rbp+var_D1], 31h ; '1'
mov [rbp+var_D0], 5Dh ; ']'
mov [rbp+var_CF], 0
lea rdx, [rbp+var_20]
lea rax, [rbp+var_10]
mov r8, rdx
mov rcx, rax
mov edx, offset aSSDevNull21 ; "%s %s >/dev/null 2>&1"
mov esi, 3FFh ; maxlen
mov edi, offset buf ; s
mov eax, 0
call _sprintf
mov edi, offset buf
call executecmd
test eax, eax
jz short loc_40FE5
```

There are a few potential insecure coding errors in this code:

1. Variable injection: The `$device_id` variable is taken directly from `$REQUEST['device_id']` without any input validation or sanitization. This could allow an attacker to inject malicious code or data into the application.
2. Command injection: The `exec` function is used to execute a system command with the `$device_id` variable as a parameter. If the `$device_id` variable is not properly sanitized, this could allow an attacker to inject malicious code into the system command and execute arbitrary code on the server.
3. Cross-site scripting (XSS): The `$SESSION['csrf-token']` variable is not properly sanitized before being output to the page in the `toggle_alignment` function. This could allow an attacker to inject malicious code into the page and steal sensitive user data.

To address these issues, it is recommended to:

1. Validate and sanitize any input variables, including `$device_id`.
2. Use parameterized queries or escape user input when constructing system commands to prevent command injection attacks.
3. Properly sanitize any user input before outputting it to the page to prevent XSS attacks.



IT'S NOT AI AND IT WON'T TAKE OUR JOBS (YET)

- ChatGPT hallucinates like a VC bro at Burning Man
- No recognition of code interdependencies & imports
- Automated SAST is not reliable; tons of false positives
- Token limitations/price
- Too slow for at-scale analysis
- GPT3 >> GPT4
- Custom LLMs?



```
==> gnssAutoAlign.php

[*] AI-Assisted analysis for ./logs/firmware/unblob_extracted/firmware_extract/191-31707726.zip_extract/gzip.uncompressed_extract/home/www-data/admin/
gnssAutoAlign.php (-rw-r--r-- root root)

[*] AI-assisted analysis results via OpenAI ChatGPT:
"Potential vulnerabilities and exploits in the code:

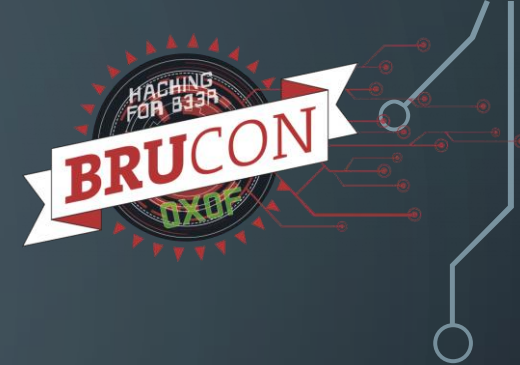
1. In line 16, the value of the \"device_id\" parameter obtained from the user input ($_REQUEST['device_id']) is directly used in the file paths without any validation or sanitization. This can lead to path traversal attacks, allowing an attacker to access arbitrary files on the server by manipulating the \"device_id\" parameter.
```

```
==> gnssAutoAlign.php

[*] AI-Assisted analysis for ./logs/firmware/unblob_extracted/firmware_extract/191-32165988.zip_extract/gzip.uncompressed_extract/home/www-data/admin/
gnssAutoAlign.php (-rw-r--r-- root root)

[*] AI-assisted analysis results via OpenAI ChatGPT:
"This code snippet has several potential vulnerabilities:

1. In line 4, the value of `device_id` is taken directly from the user input `$_REQUEST['device_id']` without any form of validation or sanitization. This could allow an attacker to inject malicious data, such as special characters or SQL injection code, leading to a potential security issue.
```



ADJACENT RESEARCH

ONEKEY - SECURITY ADVISORY:

NETMODULE INDUSTRIAL ROUTERS VULNERABLE!

Security Advisory: Multiple Vulnerabilities in NetModule Routers

February 24, 2023

ONEKEY - SECURITY ADVISORY:

PHOENIX CONTACT ROUTERS ACCESS VULNERABILITIES FOUND!

Security Advisory: Multiple Vulnerabilities in Phoenix Contact Routers

March 28, 2023

Code analysis: command injection

Confidence **MODERATE**

Command injection

Source
gnssAutoAlign.php
On line 36

Propagator 1
gnssAutoAlign.php
On line 36

Problem
gnssAutoAlign.php
On line 36

```
firmware.bin_extract/...img_extract/171-29990134.gzip_extract/171-29990134_extract/home/www-data/admin/

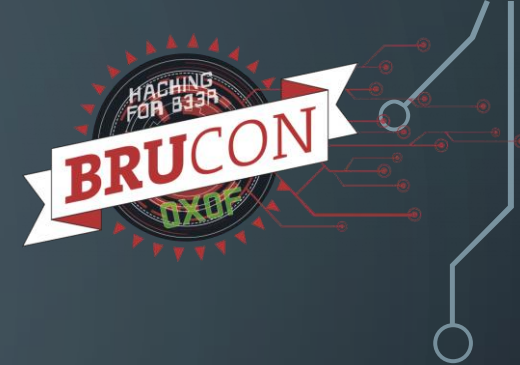
26
27     $angles = explode("\n", $angles);
28     $yaw = explode("yaw: ", $angles[0])[1];
29     $pitch = explode("pitch: ", $angles[1])[1];
30     $roll = explode("roll: ", $angles[2])[1];
31
32 }
33
34 if (isset($_POST['toggleAlignment'])) {
35     if ($status == "disabled") {
36         exec("/usr/local/sbin/www-scripts/varsious/doAutoAlignment " . $device_id . " > /dev/null &");
37     }
38     else {
39         exec("kill $(cat ". PID_FILENAME . ")");
40         $status = "stopping";
41     }
42 }
43 }
44
45 if (isset($_REQUEST['periodicUpdate'])) {
46     if (isset($pageIndex) && isset($subIndex)) {
```

```
/logs/firmware/firmware_binwalk_emba/_BF.extracted/home/www-data/admin/gnssAutoAlign.php
external.semgrep-rules.php.lang.security.exec-use
Executing non-constant commands. This can lead to command injection.

36| exec("/usr/local/sbin/www-scripts/varsious/doAutoAlignment " . $device_id . " > /dev/null &");
40| exec("kill $(cat ". PID_FILENAME . ")");
```




Now is not the time for fear



BUSTED: UNDOCUMENTED SECURITY PATCH

- OneKey blogs reused a screenshot
- Firmware contained GUI page & httpd server
- Shodan all the things
 - 'http.title:"Web Manager" +lighttpd
- RACOM MIDGE2 industrial router
- Firmware update shortly after 2nd OneKey blog
- Update contained the exact same fix
- No CVE mentioned

Firmware - MIDGE2			
Firmware MIDGE2	midge2-fw-4.6.40.103.img	31 615 kB	2023/04/06
Firmware Release notes MIDGE2 4.6.40	midge2-fw-rn-en.pdf	453 kB	2023/04/11
MIB table	midge2-mib.mib	42 kB	2022/05/26
Zabbix ver. 6 templates	midge2-zabbix-v6.0.zip	4 459 kB	2022/05/26
Toby L200 (A bands) FW 17.00 A01.02 (since FW 4.6.40.103)	TOBY-L200-A-FW17.00A01.02.tar.gz	24 668 kB	2023/04/06
Toby L210 (E bands) FW 17.00 A01.02 (since FW 4.6.40.103)	TOBY-L210-E-FW17.00A01.02.tar.gz	24 668 kB	2023/04/06
Toby L280 (P bands) FW 17.00 A01.02 (since FW 4.6.40.103)	TOBY-L280-P-FW17.00A01.02.tar.gz	24 667 kB	2023/04/06

SHODAN Explore Downloads Pricing `http.title:"Web Manager" +lighttpd`

TOTAL RESULTS
180

TOP COUNTRIES

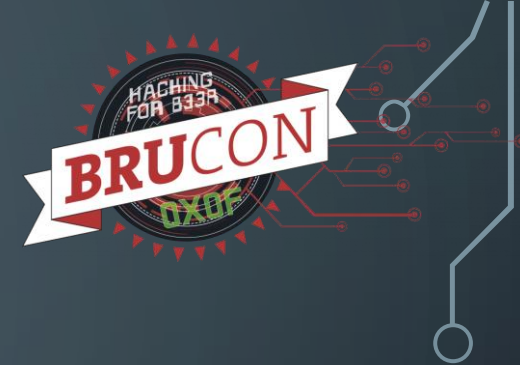
View Report Download F

Product Spotlight: Free, Fast

Netbox Web Manager
46.74.67.115
046074067115.atmpu0003.highwa
y.a1.net
A1 Telekom Austria AG
Austria, Vienna
self-signed

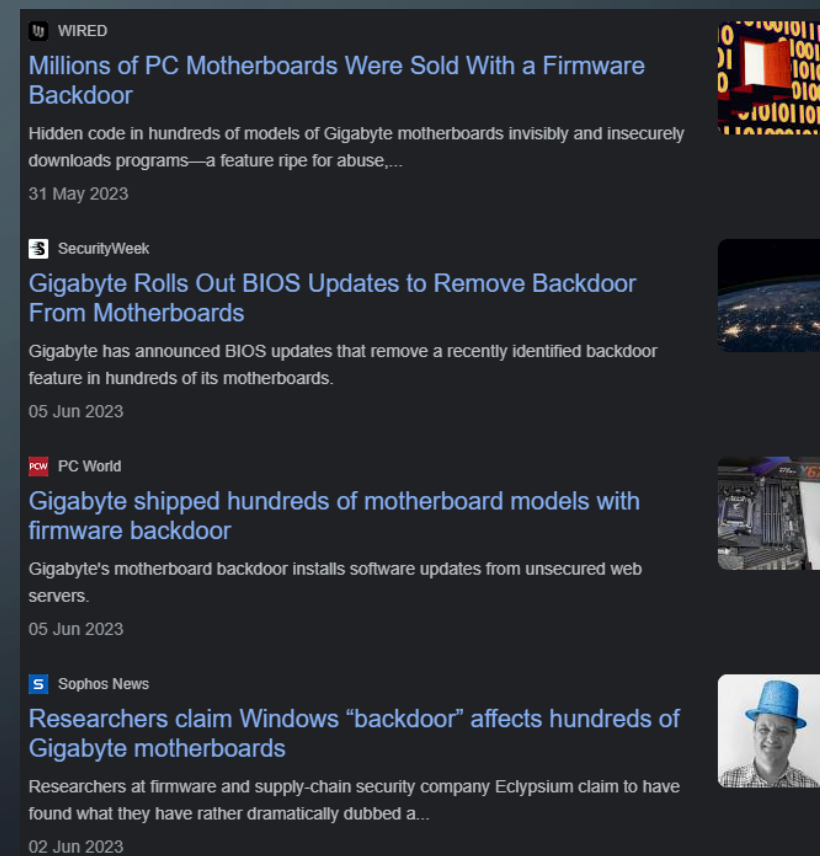
Web Manager
77.16.10.222
77.16.10.222.tmi.telenormobil.no
Telenor Norge AS
Norway, Mundal

NB2700 Web Manager



HOW NOT TO BUILD A BACKDOOR

- Initially detected as Cr4sh/SmmBackdoor
- Windows binary embedded in UEFI
- Written to disk on Windows startup
- Registers binary as a service
- Dropped binary then retrieves payloads
- No signature validation
- No certificate pinning
- Same technique as LoJax, MosiacRegressor, MoonBounce





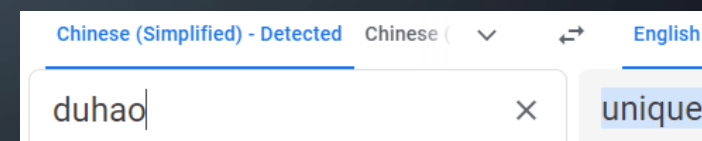
(IN)SECURITY CAMERA SYSTEMS



```
root:ToC0v8qxP13qs:0:0:root:/root:/bin/sh
admin:y1VXjXdLpGfug:0:0:admin:/bin/sh
root:y1NMyNaXWRwx.:0:0:root:/root:/bin/sh

Loaded 3 password hashes with 2 different salts (1.5x same-salt boost)
12345      (admin)
duhao     (root)

[*] John the ripper final status: 2 password hashes cracked, 1 left
[+] Password hash cracked: admin:12345:0:0:admin:/bin/sh
[+] Password hash cracked: root:duhao:0:0:root:/bin/sh
```



- Hikvision IP cameras
- Paid engagement for a government contractor
- Hardcoded passwords on 2 accounts
- Second proposed engagement ... also Hikvision
- SSH host key backdoor



```
[+] Warning: Possible authorized_key backdoor detected: /logs/firmware/unblob_extracted/
/etc/defconfig/user_home/keymgmt/.ssh/authorized_keys (-rw-r--r-- root root)
[+] Warning: Possible authorized_key backdoor detected: /logs/firmware/unblob_extracted/
/etc/defconfig/user_home/mgmt/.ssh/authorized_keys (-rw-r--r-- root root)
[+] Warning: Possible authorized_key backdoor detected: /logs/firmware/unblob_extracted/
/etc/defconfig/user_home/solusr/.ssh/authorized_keys (-rw-r--r-- root root)
```

THIS IS WHY WE CAN'T HAVE NICE THINGS, DARLING

- Shellshock (!)
- Heartbleed
- Default creds *everywhere*
- SMB vulns in network DVRs
- Linux 2.x & 3.x kernels

```
[+] Identified 763 CVE entries.
    Identified 317 High rated CVE entries / Exploits: 117
    Identified 411 Medium rated CVE entries / Exploits: 70
    Identified 35 Low rated CVE entries / Exploits: 12
    199 possible exploits available (3 Metasploit modules).
    Remote exploits: 0 / Local exploits: 4 / DoS exploits: 1 / Github PoCs: 195
```



Firmware Analysis and Comparison Tool
Home
Database
Upload
Info
Feedback

Download
Analysis
Admin
Comparisons

Lantronix G520 v. 1.9.0R10

Private Key Found
critical CVE
Linux Kernel 5.4.41
Password: admin:admin

UID: b9e5ffd50592486147f0539bef4ff71e5d2b27685f4be882976baf95ee586835_36125696

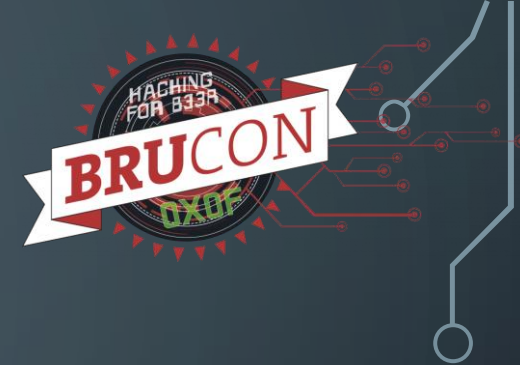
Firmware Analysis and Comparison Tool
Home
Database
Upload
Info
Feedback

Download
Analysis
Admin
Comparisons

Digicap Digicap_V5.2.0build181123 v. V5.2.0

Password: admin:12345
critical CVE
Linux Kernel 3.0.8
Heartbleed
Private Key Found

UID: c968901a6f9f612788dccc9a37c4f3844e099bcb86301e332d5b48938819d973_43279058



BECAUSE YOU BREAK THEM

- Serial to Ethernet devices
- Passwordless accounts
- Shell scripts as shells
- Passwords displayed in banner
- 9 root accounts?
- ping \$1

SHODAN Explore Downloads Pricing lantronix password: -secured

TOTAL RESULTS
1,215

TOP COUNTRIES

United States	848
Canada	74
Czechia	57
Sweden	32
United Kingdom	29

View Report Download Results Historical Trend

Partner Spotlight: Looking for a place to store all the Shodan d

66.183.177.76
s66-183-177-76.bc.hsia.telus.net
TELUS Communications Inc.
Canada, Vancouver

*** Lantronix UD51100 Device Server
MAC address 0080A3833FD0
Software version V6.11.0.0 (150500)
Password :

128.95.105.9
University of Washington
United States, Seattle

Lantronix:
Type: X90
Version: 6.10.0.1
MAC Address: 00:80:A3:84:BE:5D
IP Address: 128.95.105.9
Gateway: 128.95.105.100
Password: 4079



```
root:P80k8VVVqFTsM:0:0:root:/root:/bin/sh
bin:*:1:1:bin:/bin:/bin/sh
daemon:*:2:2:daemon:/usr/sbin:/bin/sh
adm:*:3:4:adm:/adm:/bin/sh
sync:*:5:0:sync:/bin:/bin/sync
shutdown:*:6:11:shutdown:/sbin:/sbin/shutdown
uucp:*:10:14:uucp:/var/spool/uucp:/bin/sh
nobody:*:65534:65534:nobody:/home:/bin/sh
config:0:0:root:/:/bin/eric_config
serialconfig:0:0:root:/:/bin/eric_config_serial.sh
console:0:0:root:/:/bin/local_console.sh
unblock:0:0:root:/:/bin/eric_config_unblock.sh
changemac:0:0:root:/:/bin/eric_config_mac.sh
changesn:0:0:root:/:/bin/eric_config_sn.sh
change pdu:0:0:root:/:/bin/eric_config_pdu.sh
ping:0:0:root:/:/bin/ping.sh
reset:0:0:root:/:/bin/reboot.sh
rmoeem:0:0:root:/:/bin/rm_oem.sh
```

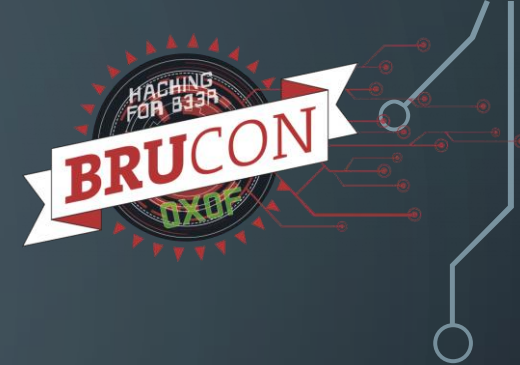

I HAD TO TAKE THEM AWAY

- Fortinet firmware is encrypted
- Fortinet firmware had zero ability verify file integrity (<v7.4.0)
- Fortinet does not support copying files to/from devices
- Forensics only performed via snapshots provided to Mandiant
- <https://bishopfox.com/blog/breaking-fortinet-firmware-encryption>



"Encryption here is not used for confidentiality because of the availability of VM images. Creating a malicious images (sic) and running it on the device is not possible because of image signing and verification." - Fortinet PSIRT

On the other hand, they promptly locked down access to firmware downloads, limiting each account to products with active licenses. As a trial user, you can now only download virtual machine images.



RESEARCH ROADBLOCKS

- Support contract requirements
- Proprietary formats
- Password protection
- Encrypted images
- Reseller-only access
- App-based updating

LILY HAY NEWMAN

SECURITY JAN 18, 2023 1:41 PM

A Widespread Logic Controller Flaw Raises the Specter of Stuxnet

More than 120 models of Siemens' S7-1500 PLCs contain a serious vulnerability—and no fix is on the way.

The vulnerability was discovered by researchers at the embedded device security firm Red Balloon Security after they spent more than a year developing a methodology to evaluate the S7-1500's firmware, which Siemens has encrypted for added protection



FIRMWARE BLIND SPOTS



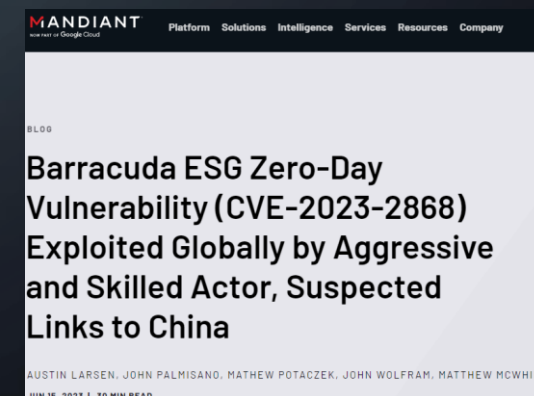


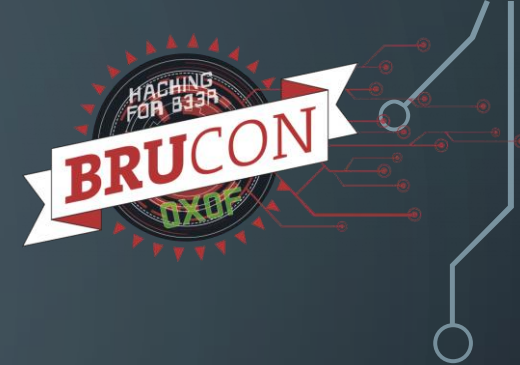
CLOSING THOUGHTS

- Everything runs firmware
- Millions of new attack points connect daily
- Firmware attacks will continue to accelerate
- Firmware controls increasingly powerful systems
- Small research community without vendor support
- Attackers will continue to have the upper hand

Table 1: Top CVEs most used by Chinese state-sponsored cyber actors since 2020

Vendor	CVE	Vulnerability Type
Apache Log4j	CVE-2021-44228	Remote Code Execution
Pulse Connect Secure	CVE-2019-11510	Arbitrary File Read
GitLab CE/EE	CVE-2021-22205	Remote Code Execution
Atlassian	CVE-2022-26134	Remote Code Execution
Microsoft Exchange	CVE-2021-26855	Remote Code Execution
F5 Big-IP	CVE-2020-5902	Remote Code Execution
VMware vCenter Server	CVE-2021-22005	Arbitrary File Upload
Citrix ADC	CVE-2019-19781	Path Traversal
Cisco Hyperflex	CVE-2021-1497	Command Line Execution
Buffalo WSR	CVE-2021-20090	Relative Path Traversal
Atlassian Confluence Server and Data Center	CVE-2021-26084	Remote Code Execution
Hikvision Webserver	CVE-2021-36260	Command Injection
Sitecore XP	CVE-2021-42237	Remote Code Execution
F5 Big-IP	CVE-2022-1388	Remote Code Execution
Apache	CVE-2022-24112	Authentication Bypass by Spoofing
ZOHO	CVE-2021-40539	Remote Code Execution
Microsoft	CVE-2021-26857	Remote Code Execution
Microsoft	CVE-2021-26858	Remote Code Execution
Microsoft	CVE-2021-27065	Remote Code Execution





REFERENCE MATERIAL

- <https://eclipsium.com/blog/vendor-re-use-opens-the-aperture-on-many-vulnerabilities/>
- <https://eclipsium.com/blog/supply-chain-risk-from-gigabyte-app-center-backdoor/>
- <https://www.welivesecurity.com/2023/03/01/blacklotus-uefi-bootkit-myth-confirmed/>
- <https://www.mandiant.com/resources/blog/fortinet-malware-ecosystem>
- <https://www.mandiant.com/resources/blog/unc3524-eye-spy-email>
- <https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally>
- <https://alperovitch.sais.jhu.edu/an-experiment-in-malware-reverse-engineering/>
- <https://securelist.com/cosmicstrand-uefi-firmware-rootkit/106973/>
- <https://research.checkpoint.com/2023/the-dragon-who-sold-his-camaro-analyzing-custom-router-implant/>
- <https://www.cisa.gov/news-events/directives/binding-operational-directive-23-02>
- https://media.defense.gov/2023/Jun/14/2003241405/-1/-1/0/CSI_HARDEN_BMCS.PDF
- <https://www.youtube.com/watch?v=6T4QsltcZ6k> (Ekoparty 2022 talk on hacking F5 & Citrix)

The background is a vibrant blue with a complex circuit board pattern. Black lines representing traces and numerous white circular pads are scattered across the surface. In the center, there is a dark blue, semi-transparent rectangular box with rounded corners. Inside this box, the text "THANK YOU BRUCON" is written in a clean, white, sans-serif font.

THANK YOU BRUCON