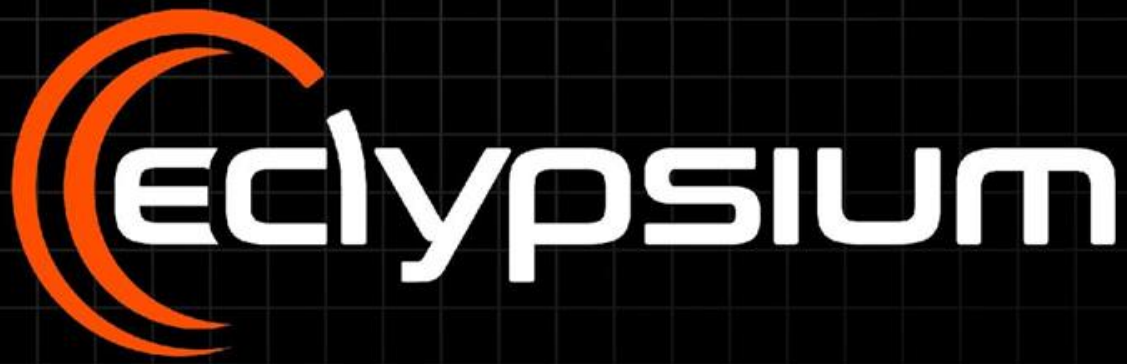


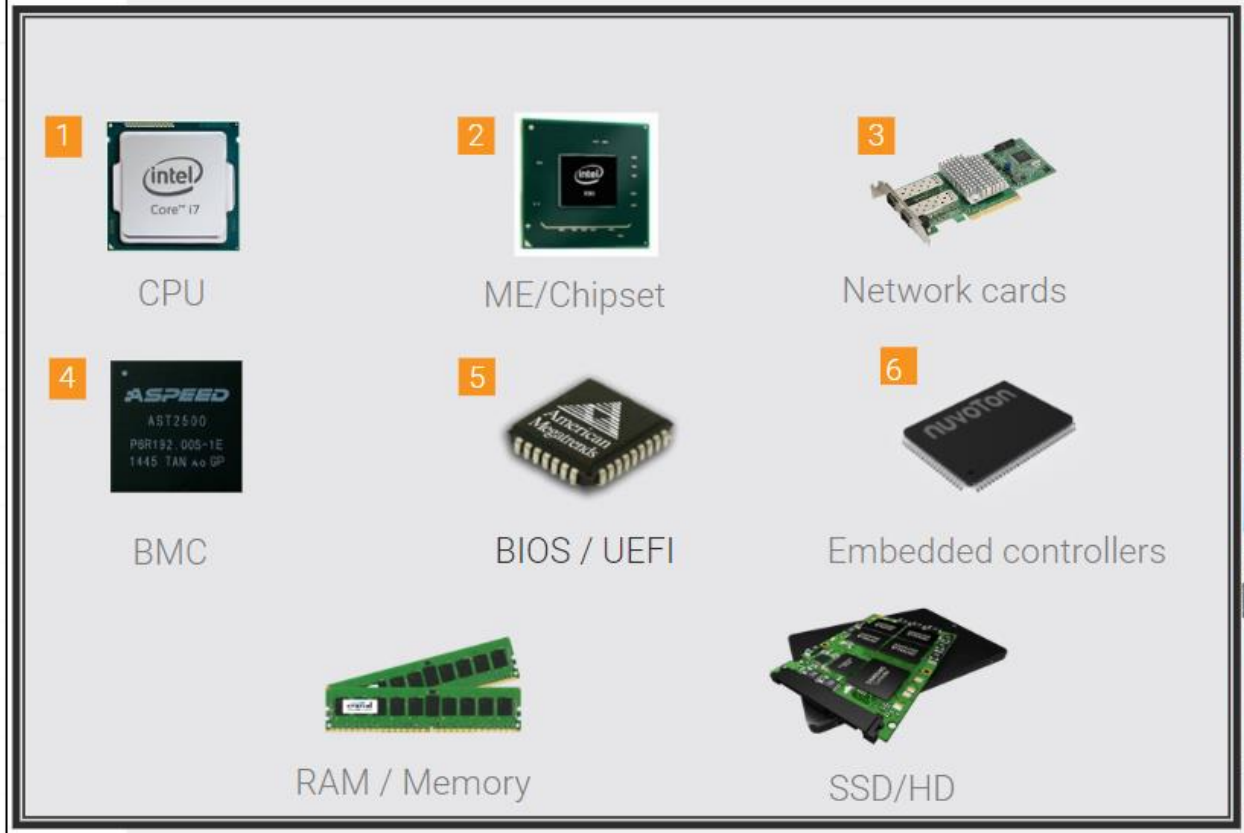
Building on Shaky Ground: Unveiling the Vulnerabilities of Firmware

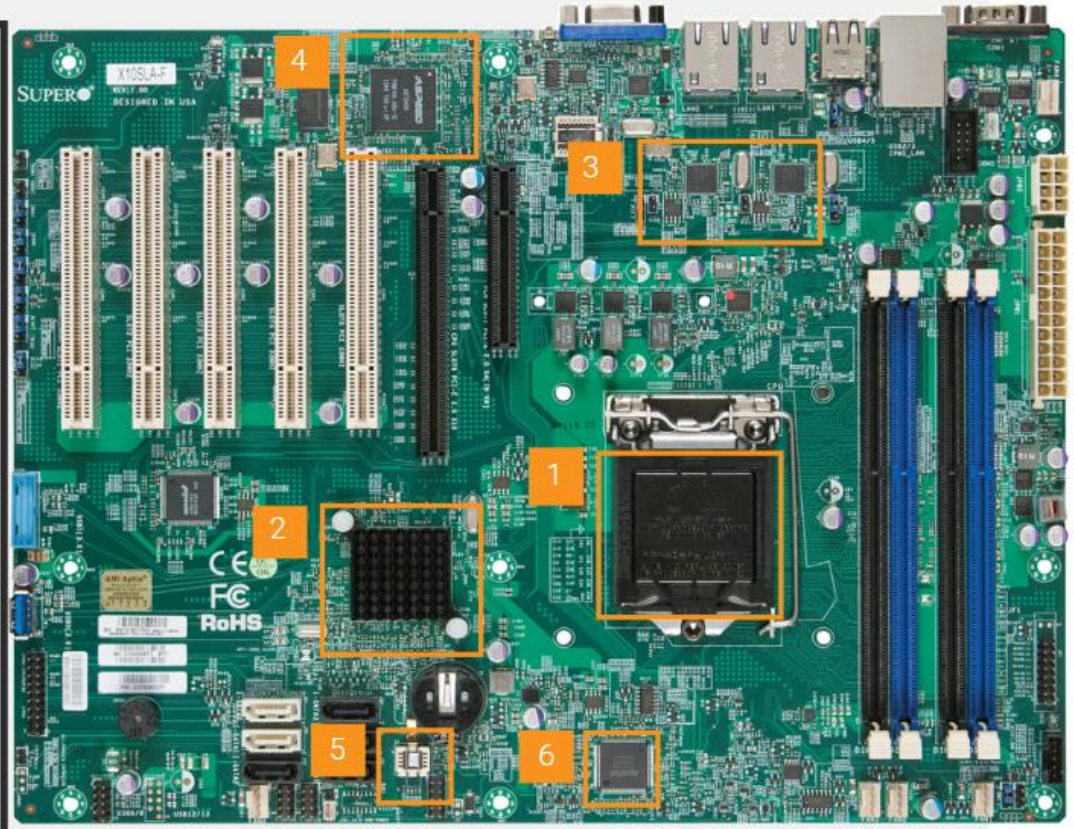
Nate Warfield
Director of Threat Intelligence & Research

/whoami

- Network hacker
- F5, Microsoft
- WIRED25 2020
- CTI League founder
- Security researcher
- Socials: @n0x08

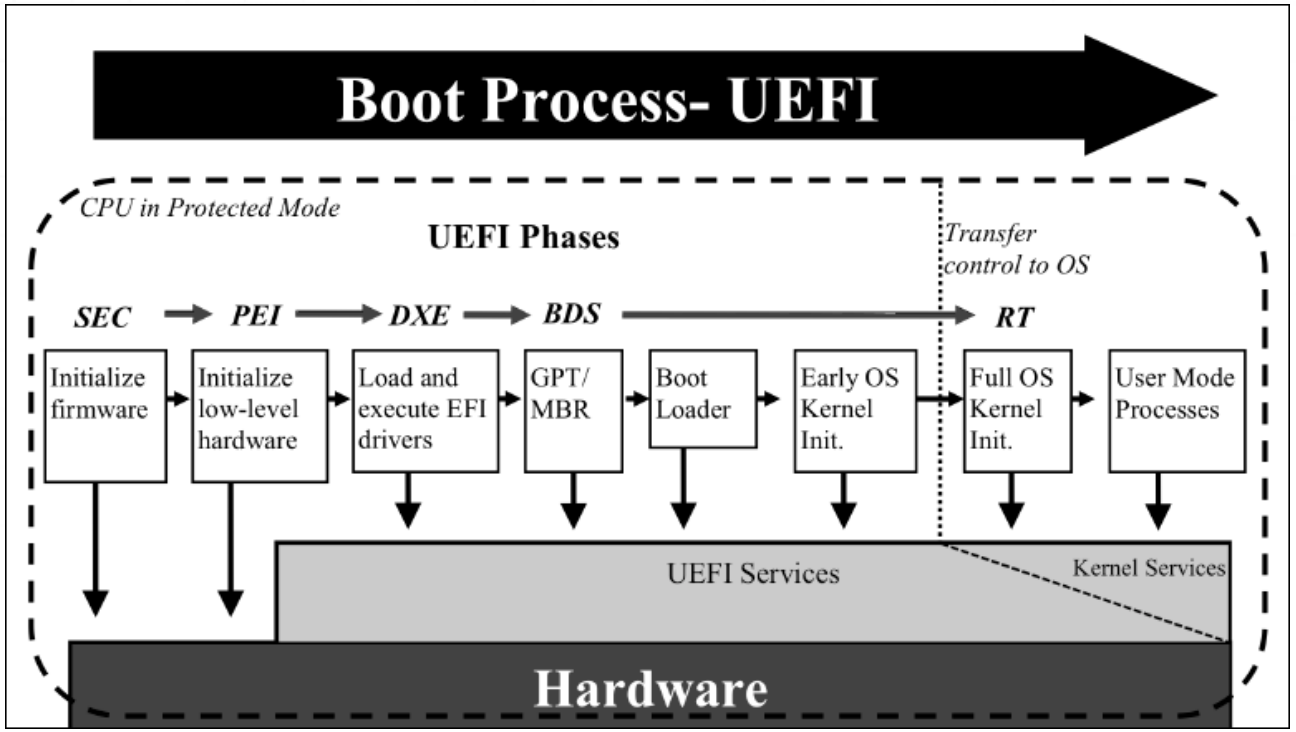
Firmware 101





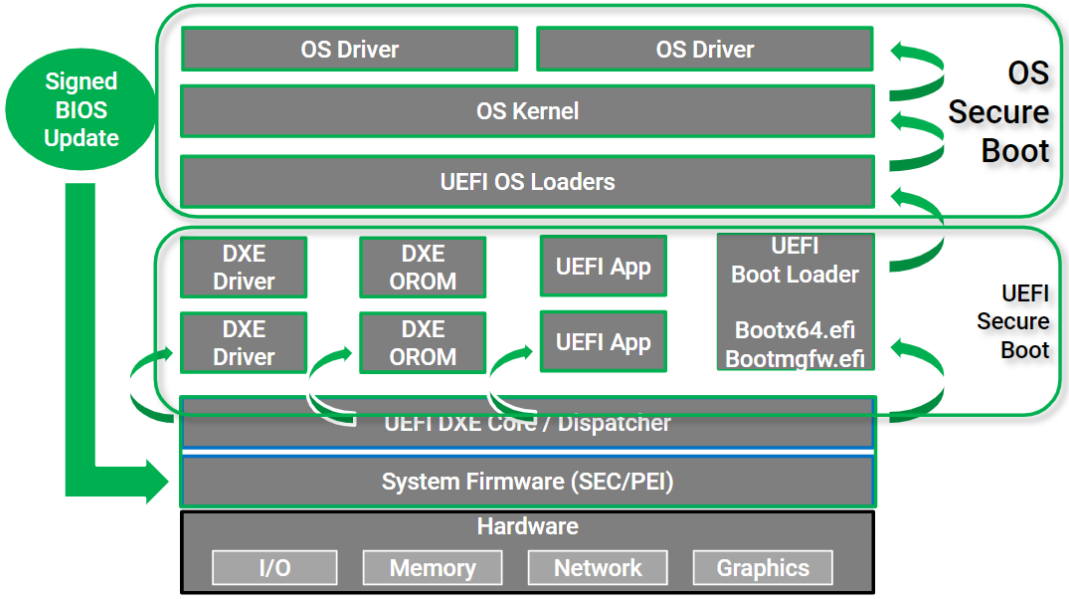
Firmware: UEFI

- Replaces BIOS
- Provides standardized boot process
- GUI for system settings
- Secure Boot
- CSM: Backwards compatibility
- Device initialization
- Network stack



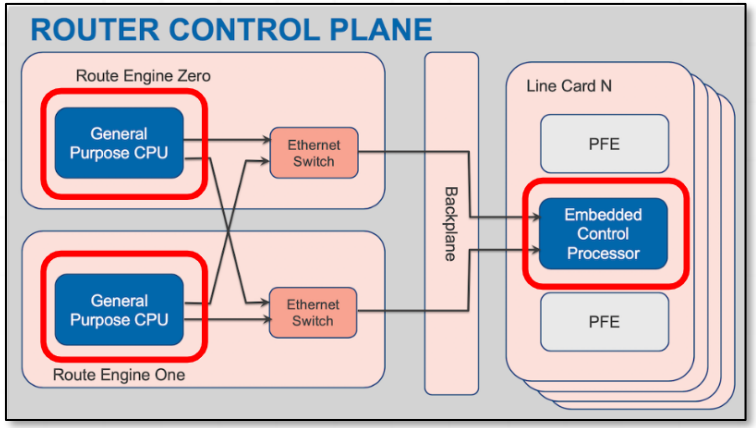
Firmware: Secure Boot

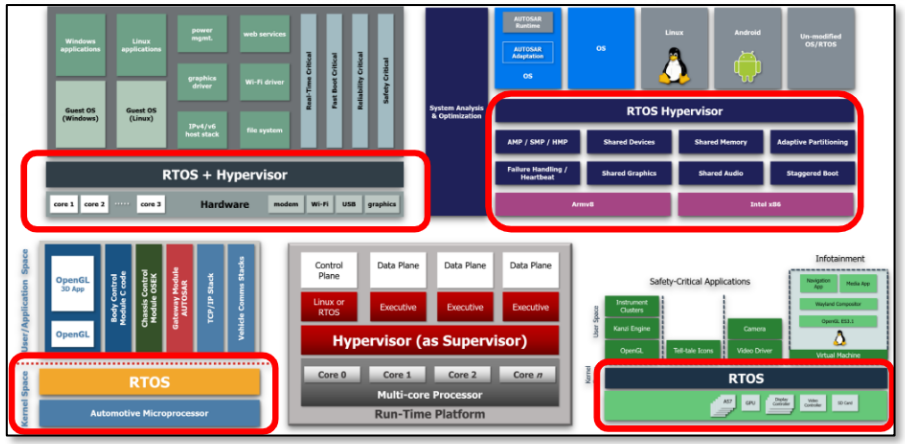
- UEFI firmware contains Platform Key (PK)
- PK signs other keys; Key Exchange Key (KEK) & Signature Database (DB) Key
- KEK ensures only trusted keys can sign software
- DB Key signs boot loaders
- During boot signatures are validated
- DBX revocation list invalidates signatures
- Vulnerable bootloaders
- Abused bootloaders



Firmware: Network devices

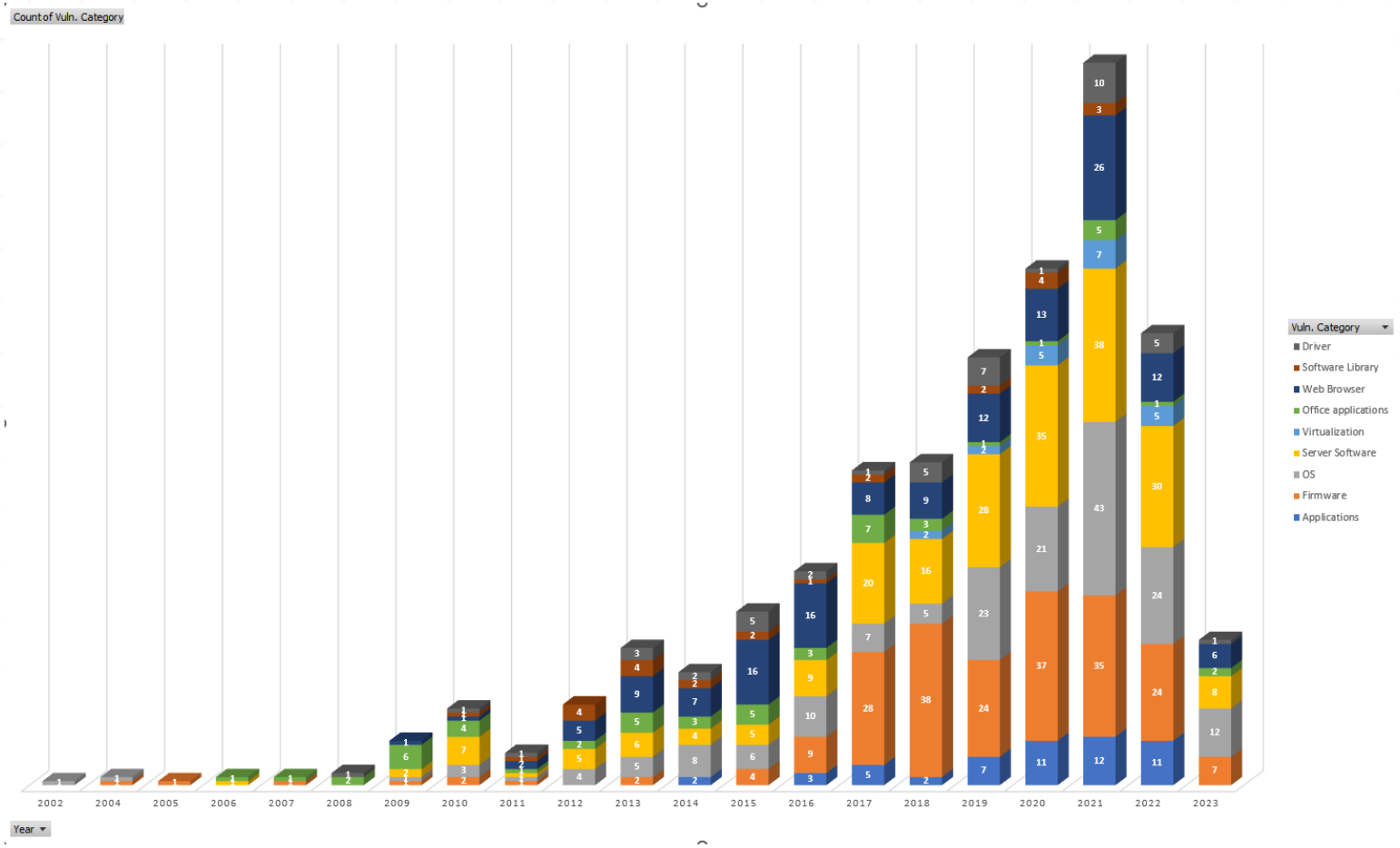
- Routers & switches
- Load balancers & firewalls
- SAN, NAS, IPTV
- Most run FreeBSD/Linux variations
- Firmware is a full operating system
- Favorite target of Nation State actors
- UNC3524; Russia (F5, Citrix)
- UNC3886; China (Fortinet)





Attackers *love* firmware

- Its old
- Frequently insecure
- Easy to exploit
- Hard to patch
- Harder to detect
- And it’s EVERYWHERE



Attacker history & timelines

2011
Mebromi
One of the first observed malware to attack the BIOS directly.

2015-2017
Equation Group & Vault 7 Leaks
Two separate instances led to tools and techniques for firmware attacks being leaked to the public. In 2015 we learned of EquationDrug and Grayfish. Later in 2017, we learned of Dark Matter and Sonic Screwdriver.

October 2020
MosaicRegressor
Researchers at Kaspersky disclosed a new UEFI implant being used in the wild dubbed MosaicRegressor. This implant has been used in targeted attacks as a way to maintain a persistent foothold in target organizations and evade most detection controls while delivering malicious payloads to compromised systems. You can find more information about MosaicRegressor and other UEFI implants here.

September 2021
FinSpy
A UEFI component belonging to the FinFisher surveillance toolset. Although researchers have tracked the spy tool since at least 2011, the bootkit didn't surface until 2021. You can find our full write-up, including a video breakdown, of FinSpy here.

January 2022
MoonBounce
Discovered in January and attributed to APT41, or an actor closely affiliated to the group, which researchers say is part of the Winnti Umbrella.

July 2022
CosmicStrand
One of the most recent examples of malware that "hooks" UEFI at an early stage to infect all subsequent operations in the boot process. The end result is malware stealthy infecting the Windows kernel, evading most protections. You can find our write-up on CosmicStrand here.

2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022

2015
Hacking Team
Hacking Team had a UEFI rootkit that was used to maintain persistent access to target systems. It is believed that this was installed with physical access, however, it is possible that physical access was not required to implant the malware.

2018
Lojax
Russian hacking group Fancy Bear is found using a UEFI rootkit to install Lojax, independent of the kernel and operating system, even a complete wipe of the hard drive will not remove the malware (patched UEFI modules of the LoJack anti-theft software (also known as Computrace) were used). (You can find our discussion of LoJax here.)

December 2020
Trickboot
Trickbot contains code to read, write, and erase firmware dubbed Trickboot. This was discovered in a collaborative research effort between Advanced Intelligence (AdvIntel) and Eclypsium.

October 2021
ESpecter
A bootkit persisting in the EFI System Partition that can bypass Windows Driver Signature Enforcement to load its own unsigned driver. You can find our article on detecting ESpector (and FinSpy) here.

June 2022
Conti Group Found Actively Looking For Firmware Vulnerabilities
Leaked chat logs show that the Conti ransomware group is actively looking for firmware vulnerabilities, specifically in Intel ME technologies.

October 2022
BlackLotus
Researchers observed a UEFI bootkit sold online called "BlackLotus". Commanding a $5,000 price tag the sellers claim this malware can bypass Secure Boot.

2023 in firmware

- 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 6: Barracuda advises device replacement
- June 13: Binding Operational Directive 23-02
- June 14: Harden BMCs

National Secrity 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.

Endpoints: Gigabyte Backdoor

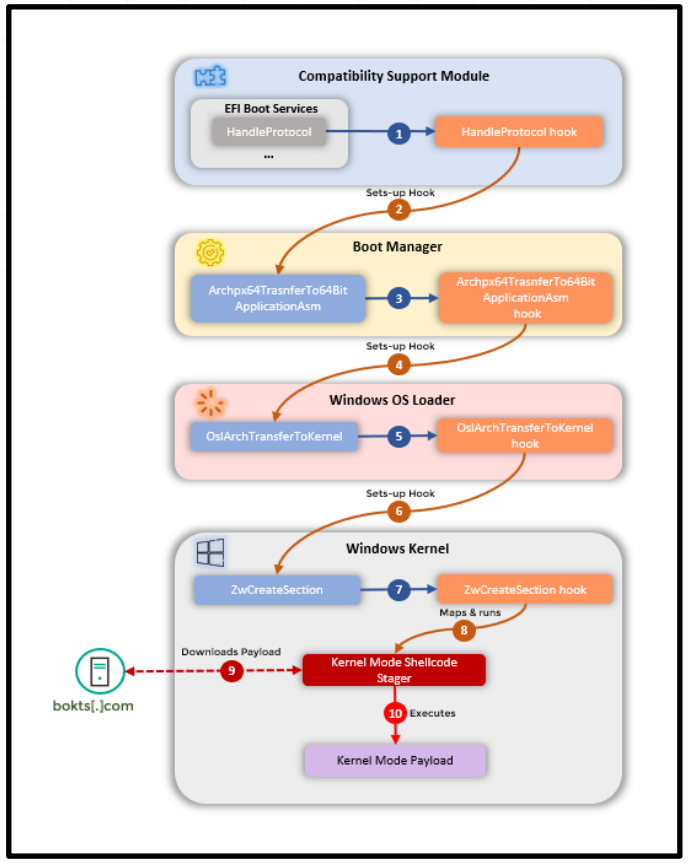
- Initially detected as Cr4sh/SmmBackdoor
- Windows binary embedded in UEFI
- Loaded into memory during boot
- Written to disk on Windows startup
- Registers binary as a service
- Dropped binary then retrieves payloads
- No signature validation
- No certificate pinning
- Same technique as LoJax, MosiacRegressor,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

README.TXT

```
  SMM backdoor for UEFI based platforms

*****************************************************************

For more information about this project please read the following article:

http://blog.cr4.sh/2015/07/building-reliable-smm-backdoor-for-uefi.html


Repository contents:

  * SmmBackdoor.py -- Python program that allows to infect PE image of UEFI DXE driver with backdoor code, communicate with
installed backdoor to read SMRAM and do some other useful things.

  * SmmBackdoor/ -- source code of UEFI part that runs in System Management Mode.

  * SmmBackdoor.efi, SmmBackdoor.pdb -- UEFI part binary and it's debug symbols.

  * smm_call/ -- proof of concept Linux program that interacts with installed backdoor to get root privileges for it's
process.
```

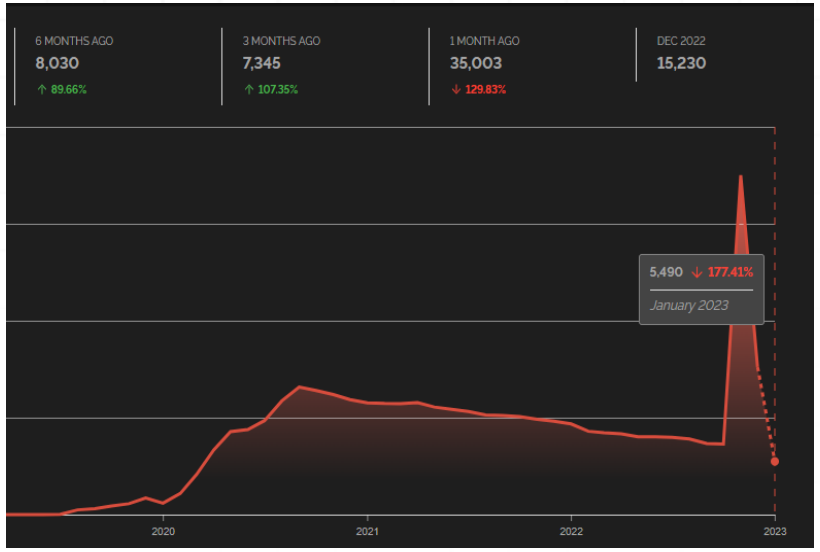
Endpoints: CosmicStrand

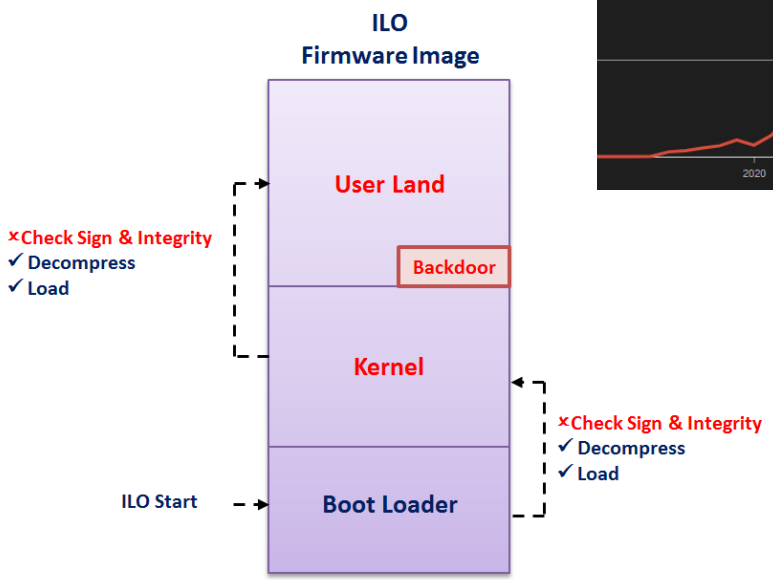
- Chinese threat actor
- Qihoo found in 2017
- Kaspersky rediscovered in 2022
- UEFI firmware rootkit
- Gigabyte & ASUS motherboards
- Hooks boot manger
- Modifies kernel loader
- Shellcode contacts C2 for secondary payload



Servers: iLOBleed

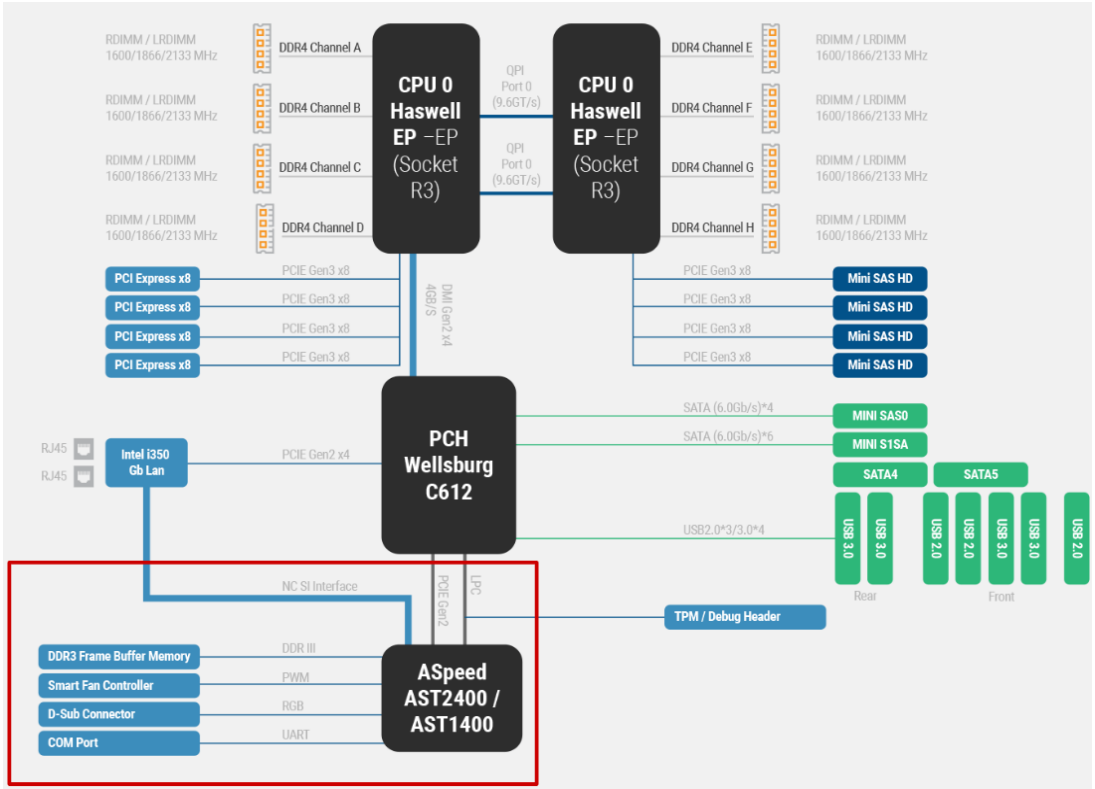
- HP integrated lights-out
- Full management control
- Accessible via iLO port OR administrative access
- Implant prevented patching
- Infected bootloader
- Disabled logging
- Disk wiping





Servers: Baseboard Management Controllers

- Platform management subsystem
- IPMI & Redfish interface
- Monitoring system hardware
- System power and reset control
- Logging and alerting
- Inventory of system components
- Virtual console (aka iKVM)
- Remote media mounting
- BIOS update



Servers: BMC&C Vulnerability Research

- CVE-2022-40259 – Arbitrary Code Execution
  via Redfish API
- CVE-2022-40242 – Default credentials for UID = 0 shell via SSH
- CVE-2022-2827 – User enumeration via API
- CVE-2022-32265 – RCE in qDecoder (fixed by maintainer)
- CVE-2022-26872 - Password reset interception via API
- CVE-2022-40258 - Weak password hashes for Redfish & API

Gigabyte Technology

https://www.gigabyte.com

Gigabyte Technology is a Taiwanese manufacturer and distributor of computer hardware. Gigabyte's principal business is motherboards.

Read more

published: 2021-08-12, visits: 834809, leak size: 46GB

WT Microelectronics

https://www.wtmec.com

WT Microelectronics Co., Ltd. develops and markets integrated circuits (IC) products. The Company's products include linear IC, applied IC, admixture semaphore IC, logic IC, image detecting IC, and memory IC. Wintech acts as an agent for Texas Instruments, Fairchild, ST Microelectronics, Marvell, Wolfson, and Bowoon.

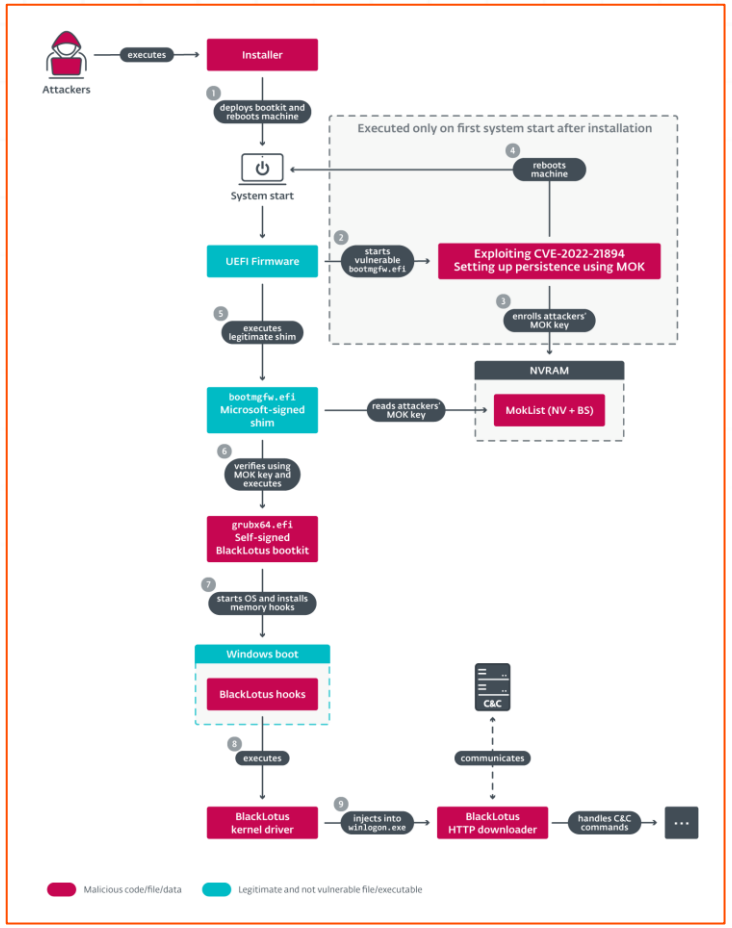
Read more

published: 2021-07-01, visits: 908085, leak size: 31.18GB

Secure Boot: BlackLotus

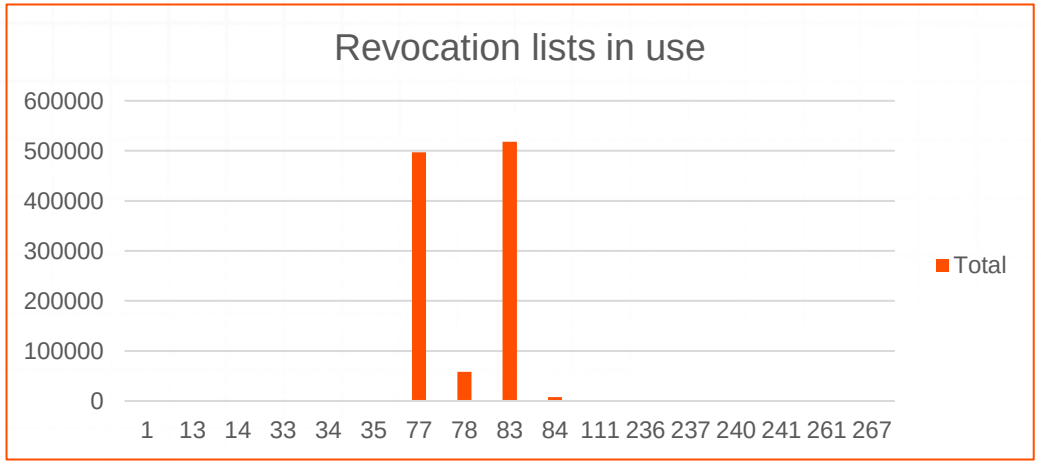
- UEFI Bootkit
- All versions of Windows 10 & 11
- Exploits Baton Drop (CVE-2022-21894)
- “Patched” in January 2022
- Patch does nothing without DBX update
- No DBX update was published, yolo
- Patch v2.0: May 2023 + DBX update
- Rolling out over multiple quarters

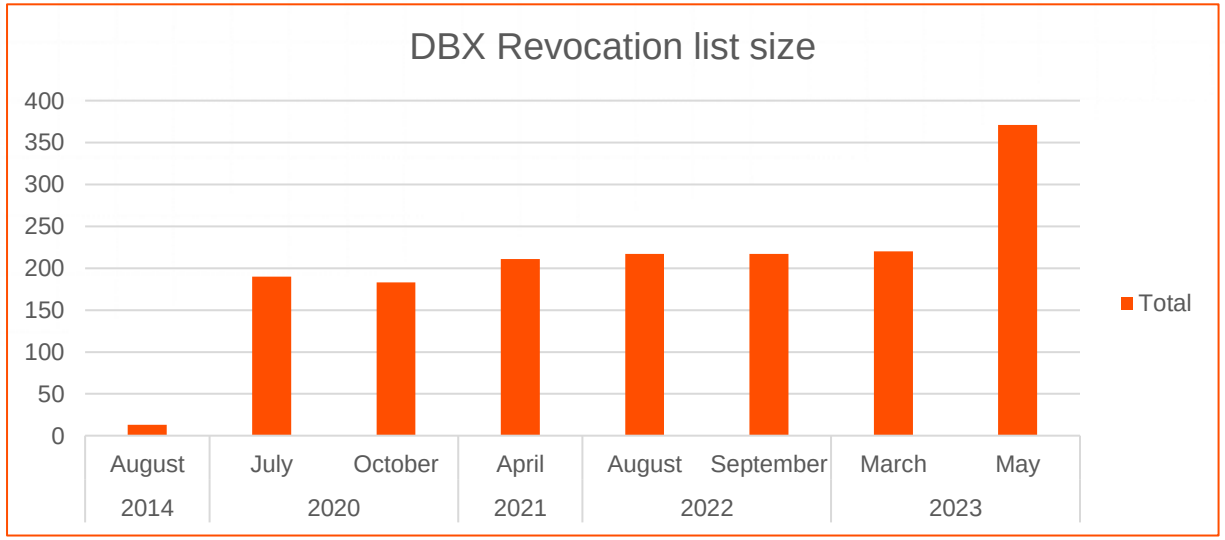
Caution: Once the mitigation for this issue is enabled on a device, meaning the revocations have been applied, it cannot be reverted if you continue to use Secure Boot on that device. Even reformatting of the disk will not remove the revocations if they have already been applied. Please be aware of all the possible implications and test thoroughly before applying the revocations that are outlined in this article to your device.



Secure Boot: 1 Million device research

- 1.1 Million dbx & dbxDefault configs analyzed
- Only 0.13% (1453) running even close to current dbx
- Origin of dbx lists likely manufacturer, too small to be UEFI.org releases
- Every system vulnerable to Black Lotus & One Bootloader attacks
- Mostly Dell, Lenovo systems



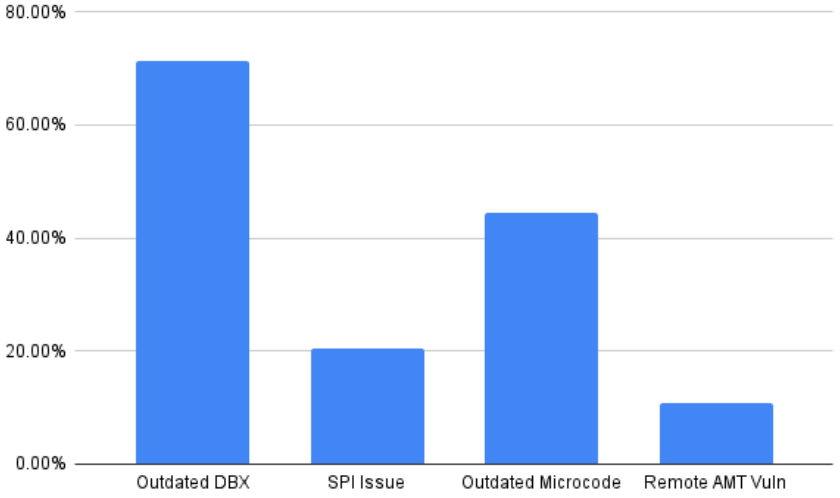


UEFI: Vulnerabilities everywhere

- 138k firmware packages
- 198k existing CVEs
- CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer is the most popular CWE
- 32k+ firmware images; 16% missing basic protections

UEFI							
# UEFI Records	AVG Code Size	AVG Image Size	AVG of Packages	AVG # of Sections	AVG # of Nodes	# Vendors	Guids
7.5M	22.4K	42.1K	5.2	4.2	1.2K	19.0	20.5K

Models				Packages		
# of Models	# Product type	# Vendors	# Firmware types	# Packages	# Avg of binaries	# Avg of models
96.9K	4.0	19.0	72.0	138.7K	417.3	10.1



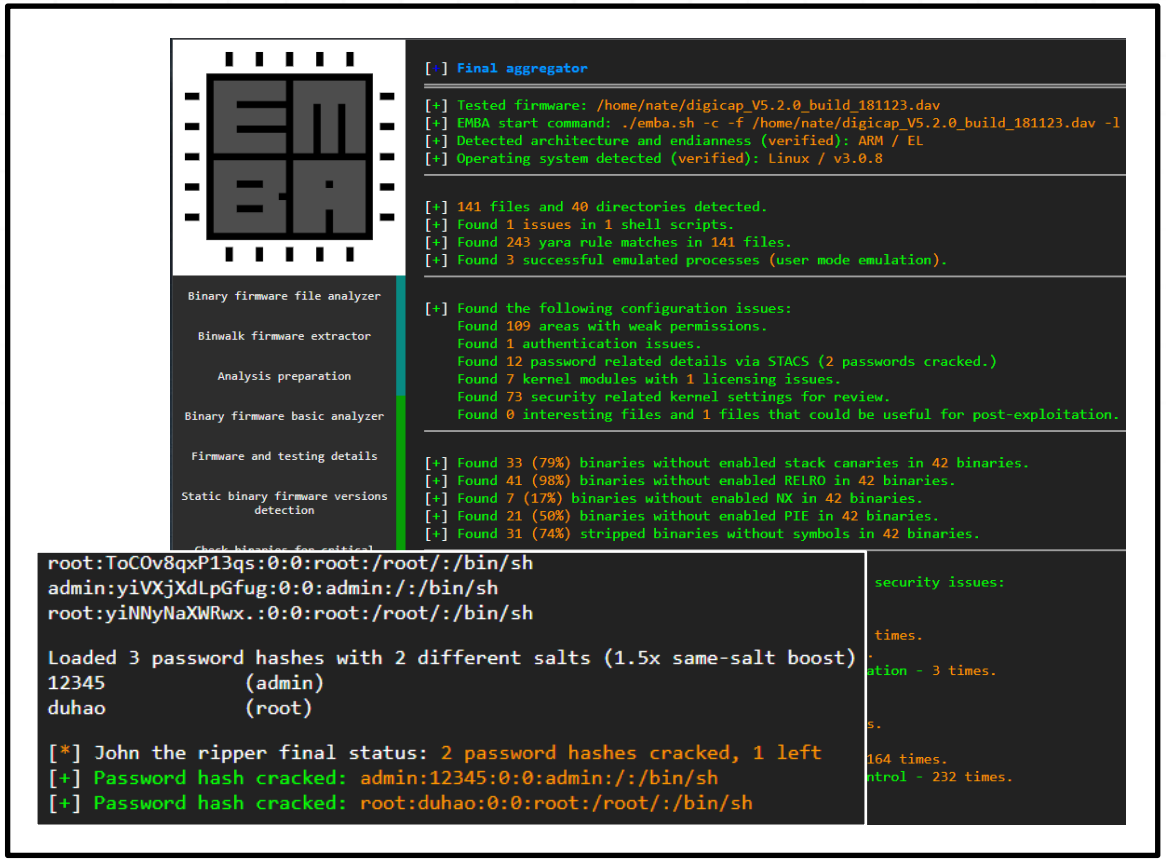
ShmooCon: “The UEFI Threat: Or How I Can “Permanently” Brick Your Computer”
https://www.youtube.com/watch?v=i70atz2o8Xc&t=8352s

FACT

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

EMBA

- No database
- CLI; web reports only
- More tests than FACT
- KEV data
- SBOM generation
- Exploit data; availability, capabilities
- Uses semgrep for SAST
- Noms CPU & RAM
- Active project, responsive developers
- My preferred tool



EMBA: Vulnerability 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 6.

Propagator 1
gnssAutoAlign.php
On line 6.

Problem
gnssAutoAlign.php
On line 36.

firmware.bin_extract/[redacted].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/various/doAutoAlignment " . $device_id . " > /dev/null &");
37          $status = "starting";
38      }
39      else {
40          exec("kill $(cat ". PID_FILENAME . ")");
41          $status = "stopping";
42      }
43  }
44
45  if (!isset($_REQUEST['periodicUpdate'])) {
46      if(!isset($pageIndx) && !isset($subIndx)) {
```

```
/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/various/doAutoAlignment " . $device_id . " > /dev/null &");
       ⋮┆----------------------------------------
      40┆ exec("kill $(cat ". PID_FILENAME . ")");
       ⋮┆----------------------------------------
```

ChatGPT for reversing & vulnerability research

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. `2Dh` 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 Copy 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    _snprintf
mov     edi, offset buf
call    executecmd
test    eax, eax
jz      loc_401AE1
```

```
mov     [rbp+var_9F], 0
mov     [rbp+var_C0], 2Dh ; '-'
mov     [rbp+var_BF], 6Bh ; '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], 6Bh ; '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    _snprintf
mov     edi, offset buf
call    executecmd
test    eax, eax
jz      short loc_400FE5
```

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

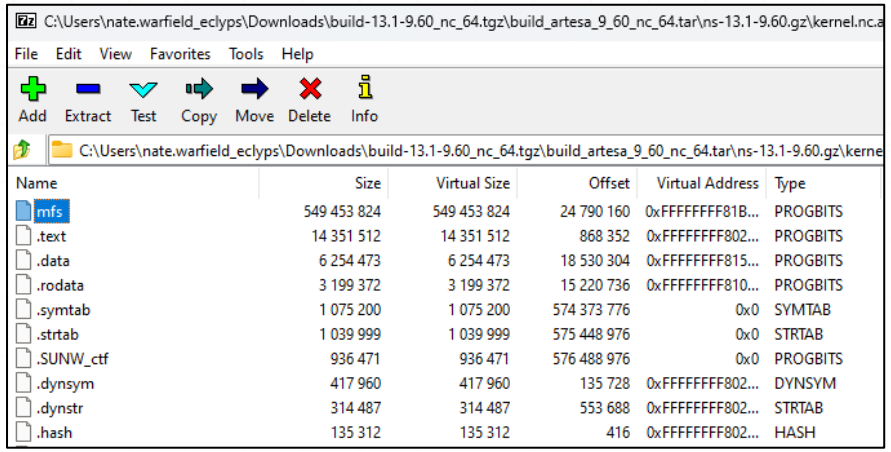
1. Variable injection: The `$device_id` variable is taken directly from `$_REQUEST['device_id']` without any input validation or sanitization. This could allow an attacker to inject malicious code or data into the application.
2. Command injection: The `exec` function is used to execute a system command 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:

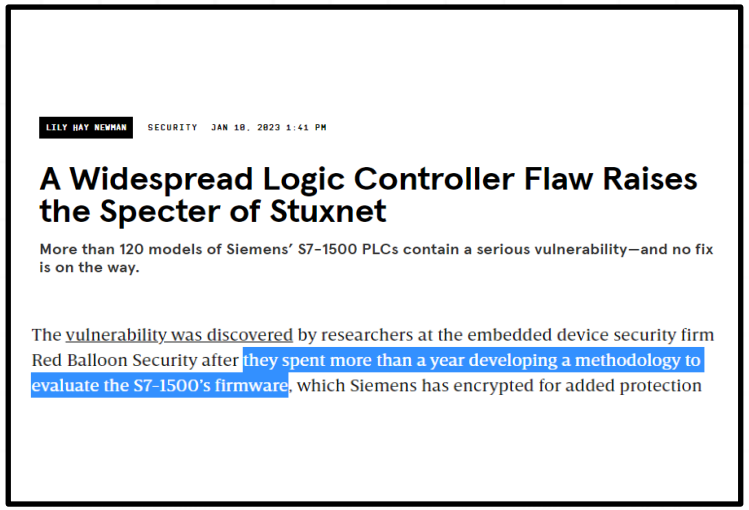
1. Validate and sanitize any input variables, including `$device_id`.
2. Use parameterized queries or escape user input when constructing system commands to prevent command injection attacks.
3. Properly sanitize any user input before outputting it to the page to prevent XSS attacks.

Research roadblocks

- **Support contract requirements**
- Embedded memory disks
- Proprietary formats
- AES-SBox
- Password protection
- Encrypted images
- Reseller-only access
- App-based updating
- VXWorks



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

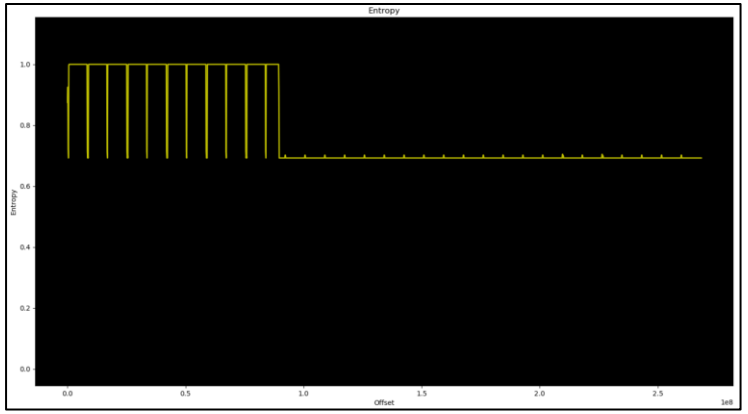


LILY HAY NEWMAN SECURITY JAN 18, 2023 1:41 PM

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



Wanna see a dead body?

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: c968901a6f9f612788dccf9a37c4f3844e099bcb86301e332d5b48938819d973_43279058


```
root:P80k8vVYqFTsM: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
```

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 UDS1100 Device Server
MAC address 0080A3B33FD0

Software version V6.11.0.0 (150508)
Password  :
```

128.95.105.9
University of Washington
United States, Seattle
ICS

```
Lantronix:
  Type: X90
  Version: 6.10.0.1
  MAC Address: 00:80:A3:B4:BE:5D
  IP Address: 128.95.105.9
  Gateway: 128.95.105.100
  Password: 4893
```

Black box vendors

APC by Schneider Electric

CRESTRON

EATON TRIPP·LITE

HID

Honeywell

Johnson Controls

Liebert

Mitel Powering connections

Raritan A brand of legrand

Closing thoughts

- Everything runs firmware
- Firmware attacks will continue to accelerate
- Millions of new attack points connect daily
- Far more security research needed on firmware
- Research is crippled by vendor policies
- Attackers will continue to have the upper hand

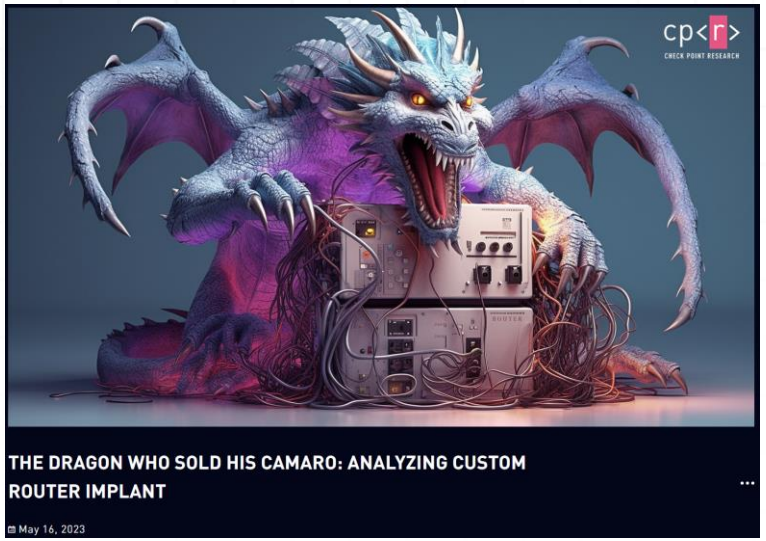


Table I: Top CVEs most used by Chinese state-sponsored cyber actors since 2020

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://eclypsium.com/blog/vendor-re-use-opens-the-aperture-on-many-vulnerabilities/
- https://eclypsium.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)

Questions?

Thank you, ISSA!