Analyzing and Modfying Firmware with Fiedka the Firmare Editor

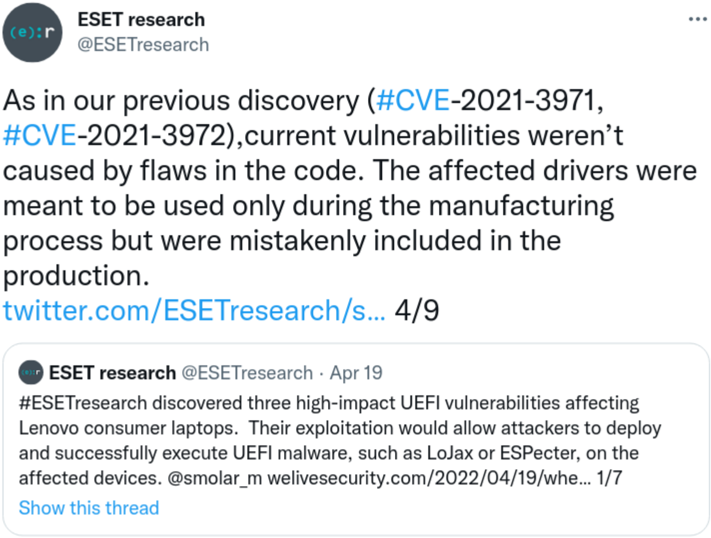
Daniel Maslowski

Agenda

- Fiedka Introduction
- Firmware Supply Chains
- Annotations and Data

Fiedka Introduction

Motivation



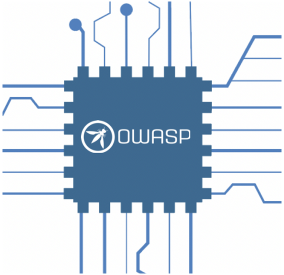
ESET research
@ESETresearch

As in our previous discovery (#CVE-2021-3971, #CVE-2021-3972),current vulnerabilities weren’t caused by flaws in the code. The affected drivers were meant to be used only during the manufacturing process but were mistakenly included in the production.
twitter.com/ESETresearch/s… 4/9

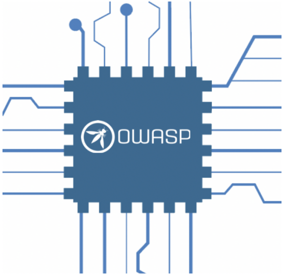
ESET research @ESETresearch · Apr 19
#ESETresearch discovered three high-impact UEFI vulnerabilities affecting Lenovo consumer laptops. Their exploitation would allow attackers to deploy and successfully execute UEFI malware, such as LoJax or ESPecter, on the affected devices. @smolar_m welivesecurity.com/2022/04/19/whe… 1/7
Show this thread

https://twitter.com/ESETresearch/status/1590279789205925888

OWASP Firmware Security Testing Methodology



OWASP Firmware Security Testing Methodology



1. Information gathering and reconnaissance
2. Obtaining firmware
3. Analyzing firmware
4. Extracting the filesystem
5. Analyzing filesystem contents
6. Emulating firmware
7. Dynamic analysis
8. Runtime analysis
9. Binary Exploitation

https://scriptingxss.gitbook.io/firmware-security-testing-methodology/

Fiedka the Firmware Editor

https://fiedka.app/

Fiedka the Firmware Editor

https://fiedka.app/

Features

- analyze firmware images
- visualize flash usage
- explore file systems
    - UEFI
    - PSP (AMD)
    - CBFS (coreboot)
- remove UEFI files
- embed LinuxBoot

Fiedka the Firmware Editor

https://fiedka.app/

Features

- analyze firmware images
- visualize flash usage
- explore file systems
    - UEFI
    - PSP (AMD)
    - CBFS (coreboot)
- remove UEFI files
- embed LinuxBoot

Work in progress

- SBoM, SWID
- annotations
- meta data export

DEMO

Let’s look at and modify an OVMF image, i.e., UEFI for virtual machines.

Firmware Supply Chains

Timeline

Timeline

2011

NIST: SP800-155 BIOS Integrity Measurement Guidelines (Draft)

> *[. . .] intended to facilitate the development of products that can detect problems with the BIOS [. . .]*

Timeline

2011

NIST: SP800-155 BIOS Integrity Measurement Guidelines (Draft)

> *[…] intended to facilitate the development of products that can detect problems with the BIOS […]*

2021

TCG: PC Client Platform

- FIM - Firmware Integrity Measurement
- RIM - Reference Integrity Manifest

Timeline

2011

NIST: SP800-155 BIOS Integrity Measurement Guidelines (Draft)

> *[…] intended to facilitate the development of products that can detect problems with the BIOS […]*

2021

TCG: PC Client Platform

- FIM - Firmware Integrity Measurement
- RIM - Reference Integrity Manifest

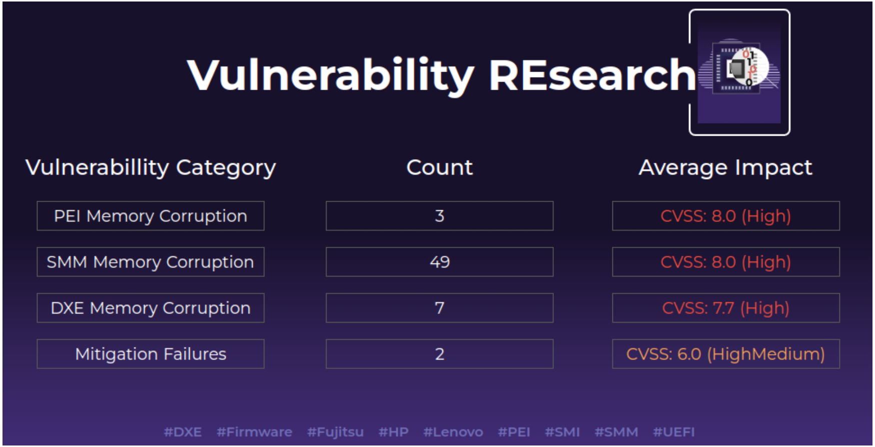
Executive Order 14028 on Improving the Nation’s Cybersecurity

- includes a lengthy definition of SBOM

> *Buyers can use an SBOM to perform vulnerability or license analysis, both of which can be used to evaluate risk in a product.*

Posted on May 12, 2021

A Host of CVEs



Vulnerability REsearch

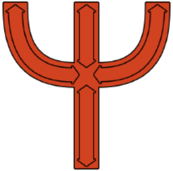
Vulnerabillity Category	Count	Average Impact
PEI Memory Corruption	3	CVSS: 8.0 (High)
SMM Memory Corruption	49	CVSS: 8.0 (High)
DXE Memory Corruption	7	CVSS: 7.7 (High)
Mitigation Failures	2	CVSS: 6.0 (HighMedium)

#DXE #Firmware #Fujitsu #HP #Lenovo #PEI #SMI #SMM #UEFI

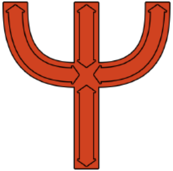
https://binarly.io/advisories

First post: July 15, 2021

Platform System Interface

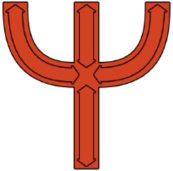


Platform System Interface



Goal: Derive a specification, summarizing firmware projects, their boot flows, how they interact as a platform with the actual operating system.

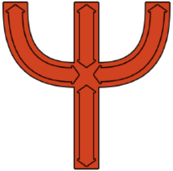
Platform System Interface



Goal: Derive a specification, summarizing firmware projects, their boot flows, how they interact as a platform with the actual operating system.

How: Extract features, compare approaches, reevaluate, improve.

Platform System Interface



Goal: Derive a specification, summarizing firmware projects, their boot flows, how they interact as a platform with the actual operating system.

How: Extract features, compare approaches, reevaluate, improve.

Example: **Auditable Firmware Implementation**

https://github.com/platform-system-interface/psi-spec/issues/4

Software Bill of Materials (SBOM)

Software Bill of Materials (SBOM)

Idea

Provide comprehensible information of what software consists of.

Software Bill of Materials (SBOM)

Idea

Provide comprehensible information of what software consists of.
Like nutrition facts, but for software.

Software Identification (SWID)

Software Identification (SWID)

https://github.com/veraison/swid

> *The swid package provides a golang API for manipulating Software Identification (SWID) Tags as described by ISO/IEC 19770-2:2015, NISTIR-8060, as well as by their “concise” counterpart CoSWID.*

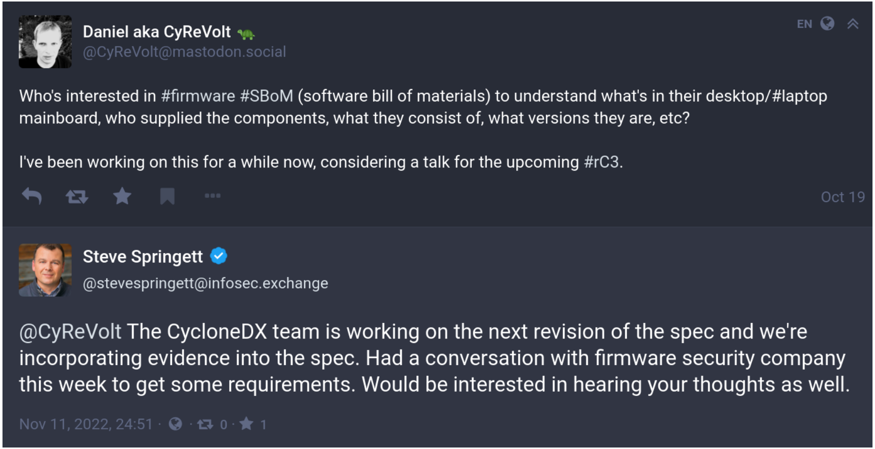
NISTIR 8060 Guidelines for the Creation of Interoperable Software Identification (SWID) Tags

http://dx.doi.org/10.6028/NIST.IR.8060

ISO/IEC 19770-2:2015 (not open/public, because ISO)

https://www.iso.org/standard/65666.html

Who’s interested?



Daniel aka CyReVolt 🐢
@CyReVolt@mastodon.social

Who's interested in #firmware #SBoM (software bill of materials) to understand what's in their desktop/#laptop mainboard, who supplied the components, what they consist of, what versions they are, etc?

I've been working on this for a while now, considering a talk for the upcoming #rC3.

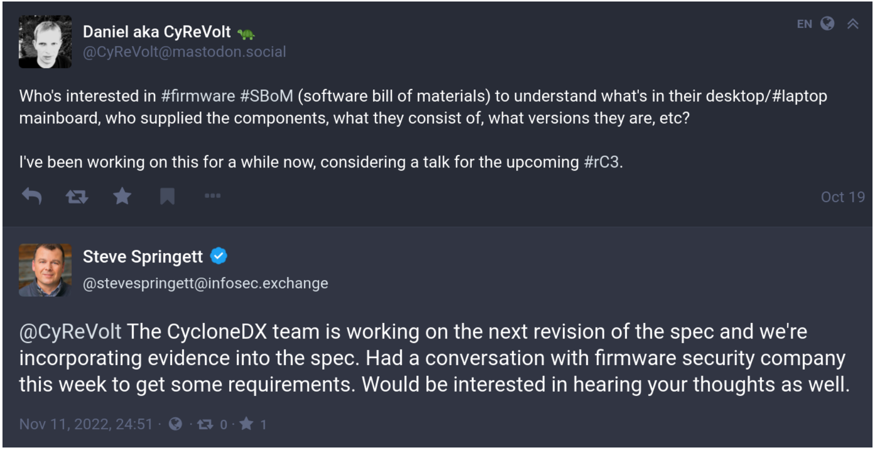
Oct 19

Steve Springett
@stevespringett@infosec.exchange

@CyReVolt The CycloneDX team is working on the next revision of the spec and we're incorporating evidence into the spec. Had a conversation with firmware security company this week to get some requirements. Would be interested in hearing your thoughts as well.

Nov 11, 2022, 24:51 · · 0 · ★ 1

Who’s interested?



Daniel aka CyReVolt 🐢
@CyReVolt@mastodon.social

Who's interested in #firmware #SBoM (software bill of materials) to understand what's in their desktop/#laptop mainboard, who supplied the components, what they consist of, what versions they are, etc?

I've been working on this for a while now, considering a talk for the upcoming #rC3.

Oct 19

Steve Springett ✓
@stevespringett@infosec.exchange

@CyReVolt The CycloneDX team is working on the next revision of the spec and we're incorporating evidence into the spec. Had a conversation with firmware security company this week to get some requirements. Would be interested in hearing your thoughts as well.

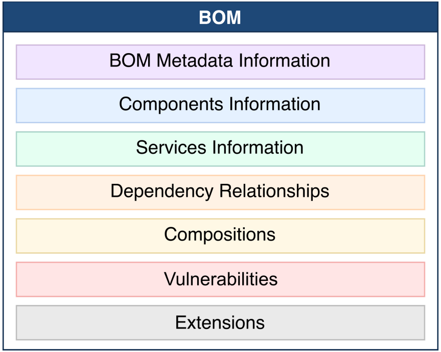
Nov 11, 2022, 24:51 · 🌐 · 🔁 0 · ★ 1

https://github.com/CycloneDX/specification/issues/129

Add evidence used to determine inclusion of a component.

OWASP CycloneDX

CycloneDX



BOM

BOM Metadata Information

Components Information

Services Information

Dependency Relationships

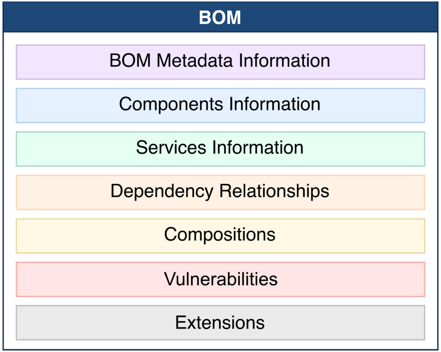
Compositions

Vulnerabilities

Extensions

OWASP CycloneDX

CycloneDX



BOM Metadata

BOM metadata includes the supplier, manufacturer, and the target component for which the BOM describes. It also includes the tools used to create the BOM, and license information for the BOM document itself.

CycloneDX Standardization

https://cyclonedx.org/about/standardization-process/

> *This is a meritocratic, consensus-based community project. Anyone with and interest in the project can join the community, contribute to the project design and participate in the decision making process.*

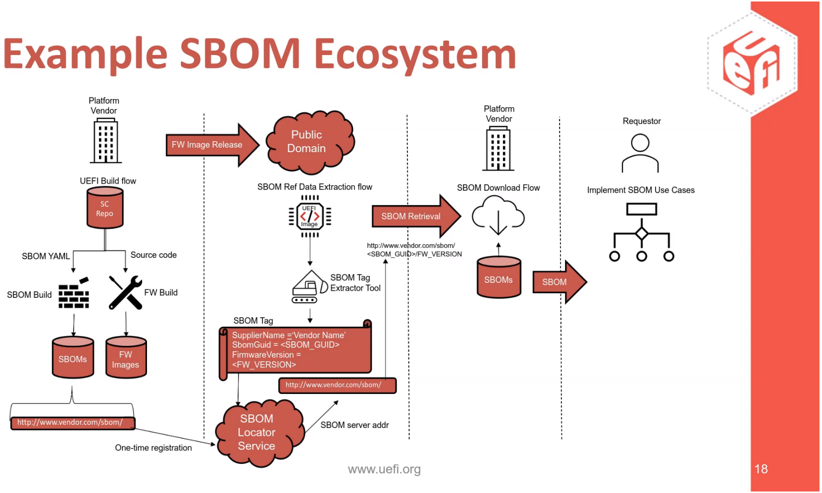
CycloneDX Standardization

https://cyclonedx.org/about/standardization-process/

> *This is a meritocratic, consensus-based community project. Anyone with and interest in the project can join the community, contribute to the project design and participate in the decision making process.*

https://github.com/CycloneDX/specification

UEFI Forum and AMI



Example SBOM Ecosystem

Platform Vendor

UEFI Build flow

SC Repo

SBOM YAML

Source code

SBOM Build

FW Build

SBOMs

FW Images

http://www.vendor.com/sbom/

One-time registration

FW Image Release

Public Domain

SBOM Ref Data Extraction flow

UEFI Image

SBOM Tag Extractor Tool

SBOM Tag

SupplierName ='Vendor Name'
SbomGuid = <SBOM_GUID>
FirmwareVersion =
<FW_VERSION>

http://www.vendor.com/sbom/

SBOM Locator Service

SBOM server addr

SBOM Retrieval

http://www.vendor.com/sbom/
<SBOM_GUID>/FW_VERSION

Platform Vendor

SBOM Download Flow

SBOMs

SBOM

Requestor

Implement SBOM Use Cases

www.uefi.org

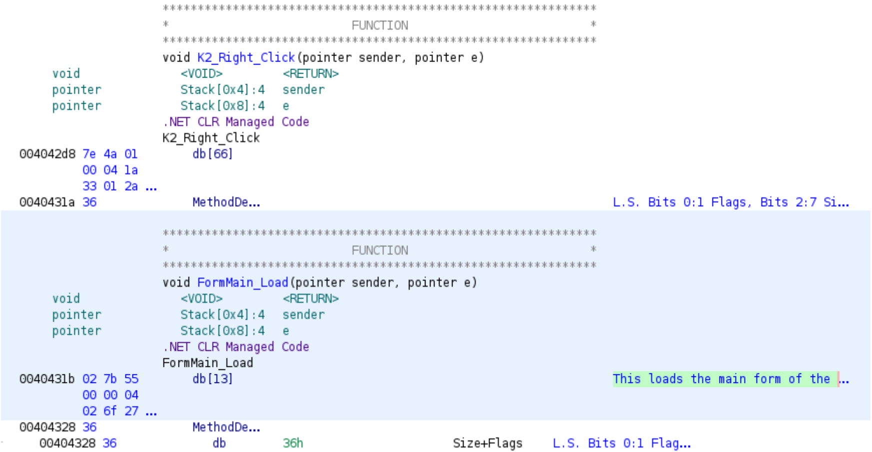
18

https://www.youtube.com/watch?v=naDYSz1a3KQ

The talk plans to address several industry-wide items necessary for a broader adoption of SBOM in the firmware ecosystem.

Annotations and Data

Ghidra

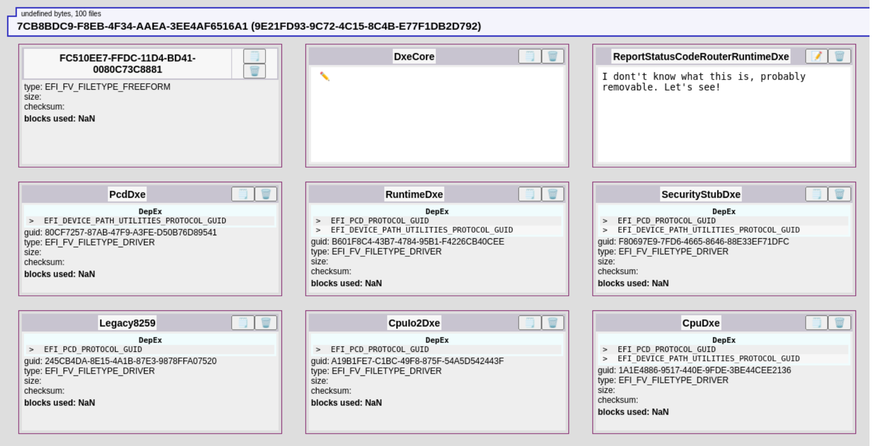


```
                         ****************************************************************
                         *                          FUNCTION                            *
                         ****************************************************************
                         void K2_Right_Click(pointer sender, pointer e)
     void                   <VOID>         <RETURN>
     pointer                Stack[0x4]:4   sender
     pointer                Stack[0x8]:4   e
                         .NET CLR Managed Code
                         K2_Right_Click
004042d8 7e 4a 01            db[66]
         00 04 1a
         33 01 2a ...
0040431a 36                  MethodDe...                                      L.S. Bits 0:1 Flags, Bits 2:7 Si...

                         ****************************************************************
                         *                          FUNCTION                            *
                         ****************************************************************
                         void FormMain_Load(pointer sender, pointer e)
     void                   <VOID>         <RETURN>
     pointer                Stack[0x4]:4   sender
     pointer                Stack[0x8]:4   e
                         .NET CLR Managed Code
                         FormMain_Load
0040431b 02 7b 55            db[13]                                           This loads the main form of the ...
         00 00 04
         02 6f 27 ...
00404328 36                  MethodDe...
   00404328 36                 db        36h                 Size+Flags    L.S. Bits 0:1 Flag...
```

Right click -> Comment -> EOL Comment -> Type -> Apply …

Fiedka



undefined bytes, 100 files

7CB8BDC9-F8EB-4F34-AAEA-3EE4AF6516A1 (9E21FD93-9C72-4C15-8C4B-E77F1DB2D792)

FC510EE7-FFDC-11D4-BD41-0080C73C8881

type: EFI_FV_FILETYPE_FREEFORM
size:
checksum:
blocks used: NaN

DxeCore

✏

ReportStatusCodeRouterRuntimeDxe

```
I dont't know what this is, probably
removable. Let's see!
```

PcdDxe

```
DepEx
>  EFI_DEVICE_PATH_UTILITIES_PROTOCOL_GUID
```

guid: 80CF7257-87AB-47F9-A3FE-D50B76D89541
type: EFI_FV_FILETYPE_DRIVER
size:
checksum:
blocks used: NaN

RuntimeDxe

```
DepEx
>  EFI_PCD_PROTOCOL_GUID
>  EFI_DEVICE_PATH_UTILITIES_PROTOCOL_GUID
```

guid: B601F8C4-43B7-4784-95B1-F4226CB40CEE
type: EFI_FV_FILETYPE_DRIVER
size:
checksum:
blocks used: NaN

SecurityStubDxe

```
DepEx
>  EFI_PCD_PROTOCOL_GUID
>  EFI_DEVICE_PATH_UTILITIES_PROTOCOL_GUID
```

guid: F80697E9-7FD6-4665-8646-88E33EF71DFC
type: EFI_FV_FILETYPE_DRIVER
size:
checksum:
blocks used: NaN

Legacy8259

```
DepEx
>  EFI_PCD_PROTOCOL_GUID
```

guid: 245CB4DA-8E15-4A1B-87E3-9878FFA07520
type: EFI_FV_FILETYPE_DRIVER
size:
checksum:
blocks used: NaN

CpuIo2Dxe

```
DepEx
>  EFI_PCD_PROTOCOL_GUID
```

guid: A19B1FE7-C1BC-49F8-875F-54A5D542443F
type: EFI_FV_FILETYPE_DRIVER
size:
checksum:
blocks used: NaN

CpuDxe

```
DepEx
>  EFI_PCD_PROTOCOL_GUID
>  EFI_DEVICE_PATH_UTILITIES_PROTOCOL_GUID
```

guid: 1A1E4886-9517-440E-9FDE-3BE44CEE2136
type: EFI_FV_FILETYPE_DRIVER
size:
checksum:
blocks used: NaN

Click on notepad button and type!

Data

Data

Why data?

- enrich analysis, exchange, gain insight
- feed back into tooling, e.g., Binarly integrated in LVFS
- back claims, e.g., regarding security and financial risks
- data drives business decisions

Data

Why data?

- enrich analysis, exchange, gain insight
- feed back into tooling, e.g., Binarly integrated in LVFS
- back claims, e.g., regarding security and financial risks
- data drives business decisions

Previous Work

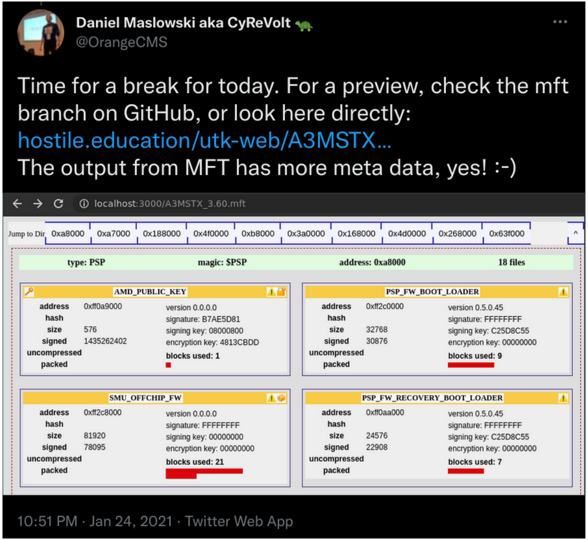
Mimoja's Firmware Toolkit for unpacking and analyzing firmware images

https://github.com/mimoja/mft

- fetchers for obtaining lots of images
- analyzers for different vendors

Mimoja's Firmware Toolkit (MFT)

Used in Fiedka prototype (utk-web) - help wanted with reintegration!



Daniel Maslowski aka CyReVolt 🐢
@OrangeCMS

Time for a break for today. For a preview, check the mft branch on GitHub, or look here directly:
hostile.education/utk-web/A3MSTX...
The output from MFT has more meta data, yes! :-)

localhost:3000/A3MSTX_3.60.mft

type: PSP **magic: $PSP** **address: 0xa8000** **18 files**

AMD_PUBLIC_KEY

address	0xff0a9000	version 0.0.0.0
hash		signature: B7AE5D81
size	576	signing key: 08000800
signed	1435262402	encryption key: 4813CBDD
uncompressed		**blocks used: 1**
packed		

PSP_FW_BOOT_LOADER

address	0xff2c0000	version 0.5.0.45
hash		signature: FFFFFFFF
size	32768	signing key: C25D8C55
signed	30876	encryption key: 00000000
uncompressed		**blocks used: 9**
packed		

SMU_OFFCHIP_FW

address	0xff2c8000	version 0.0.0.0
hash		signature: FFFFFFFF
size	81920	signing key: 00000000
signed	78095	encryption key: 00000000
uncompressed		**blocks used: 21**
packed		

PSP_FW_RECOVERY_BOOT_LOADER

address	0xff0aa000	version 0.5.0.45
hash		signature: FFFFFFFF
size	24576	signing key: C25D8C55
signed	22908	encryption key: 00000000
uncompressed		**blocks used: 7**
packed		

10:51 PM · Jan 24, 2021 · Twitter Web App

Hack all the things!