

RSA 2022

UEFI Vulnerabilities Coordination

Handling UEFI vulnerabilities
disclosure and improving UEFI
patch lifecycle

Vijay Sarvepalli

Copyright 2022 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM22-0496

Carnegie Mellon University (CMU)



Pioneering discoveries that enrich the lives of people on a global scale

- Turning disruptive ideas into success through leading-edge research
- 2021 *U.S. News and World Report* rankings:
 - #1 in computer engineering, AI, cybersecurity, and software engineering
 - #2 in overall computer science
 - #3 in data analytics/science

CMU Software Engineering Institute (SEI)



Bringing innovation to the U.S. government

- A Federally Funded Research and Development Center (FFRDC) chartered in 1984 and sponsored by the DoD
- Leader in researching complex software engineering, cyber security, and artificial intelligence (AI) engineering solutions
- Critical to the U.S. government's ability to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring

CERT Division: Birthplace of Cybersecurity



Trusted

Conducting research for the U.S. Government in a non-profit, public-private partnership

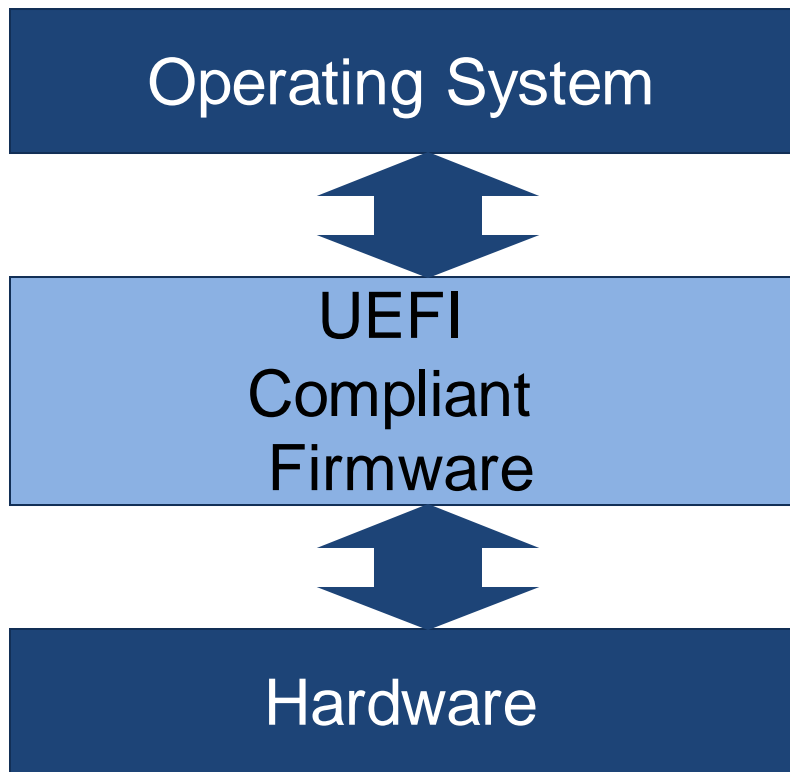
Valued

Collaborating with military, industry, and academia globally to innovate solutions

Relevant

Achieving technology and talent results for our mission partners

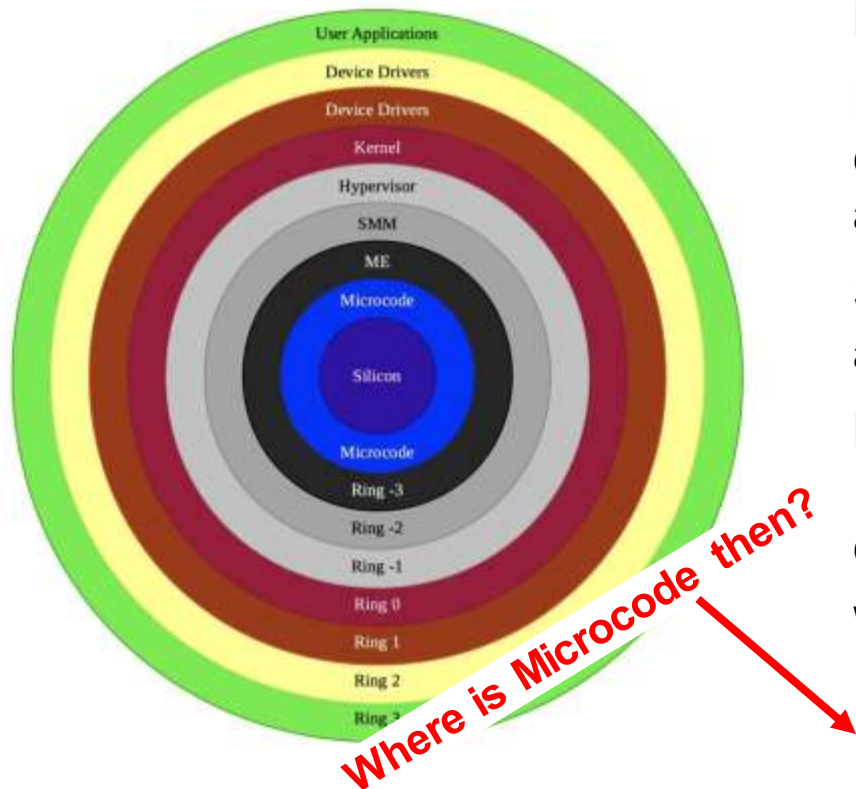
Unified Extensible Firmware Interface (UEFI)



The UEFI standard defines interface between the operating system and the firmware, which controls the hardware. This standard supersedes the legacy BIOS.

UEFI is widely used to boot and in some ways manage modern hardware.

UEFI ring of fire has many subduction zones for attacks



But in recent years there are more!

Hypervisor mode creates a new mode called Ring -1, utilized by Intel VT-x and AMD-V virtualization instructions.

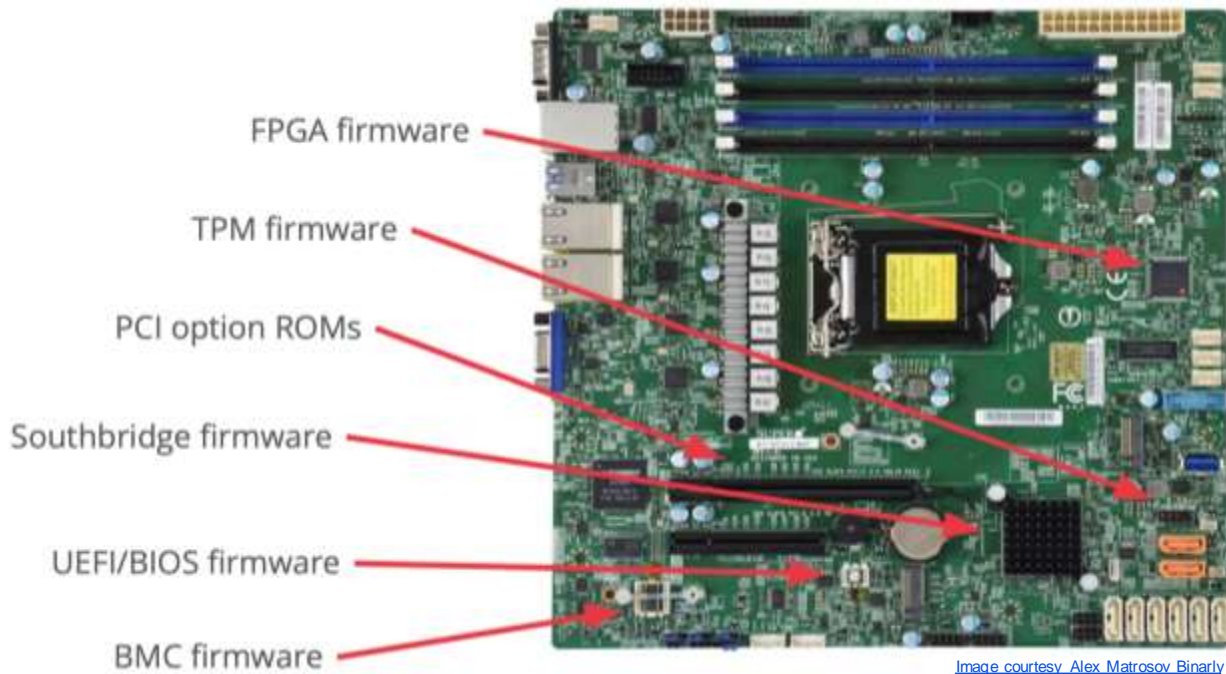
System Management Mode (SMM) adds another Ring -2.

Below that there's Intel Management Engine (ME), called Ring -3 that runs even when the computer is sleeping.

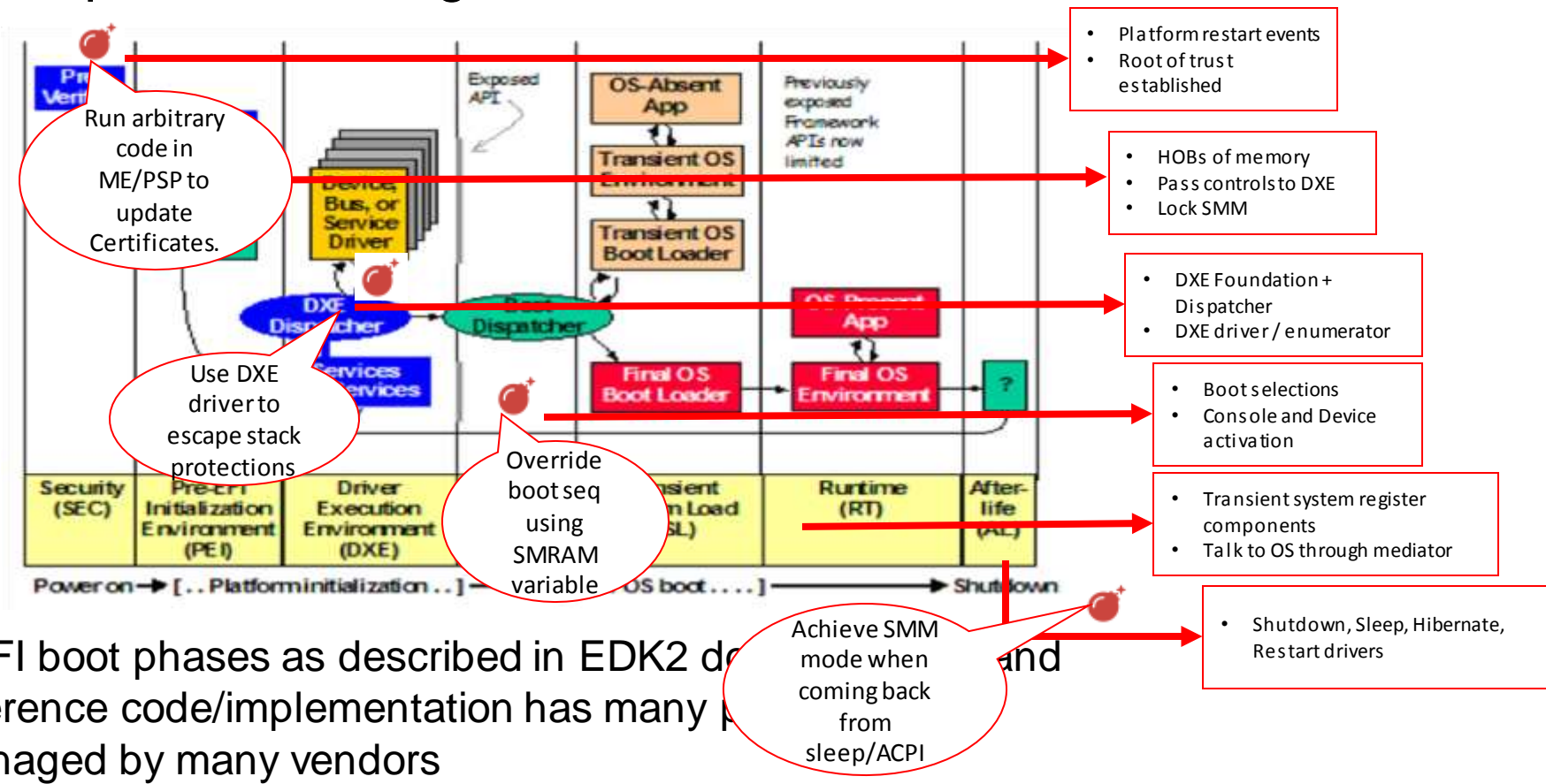
What could possibly go wrong?

- Attacker gets maximum control
- Attacker gets permanence/persistence
- OS has no visibility

Where is Firmware anyway on a modern computer?

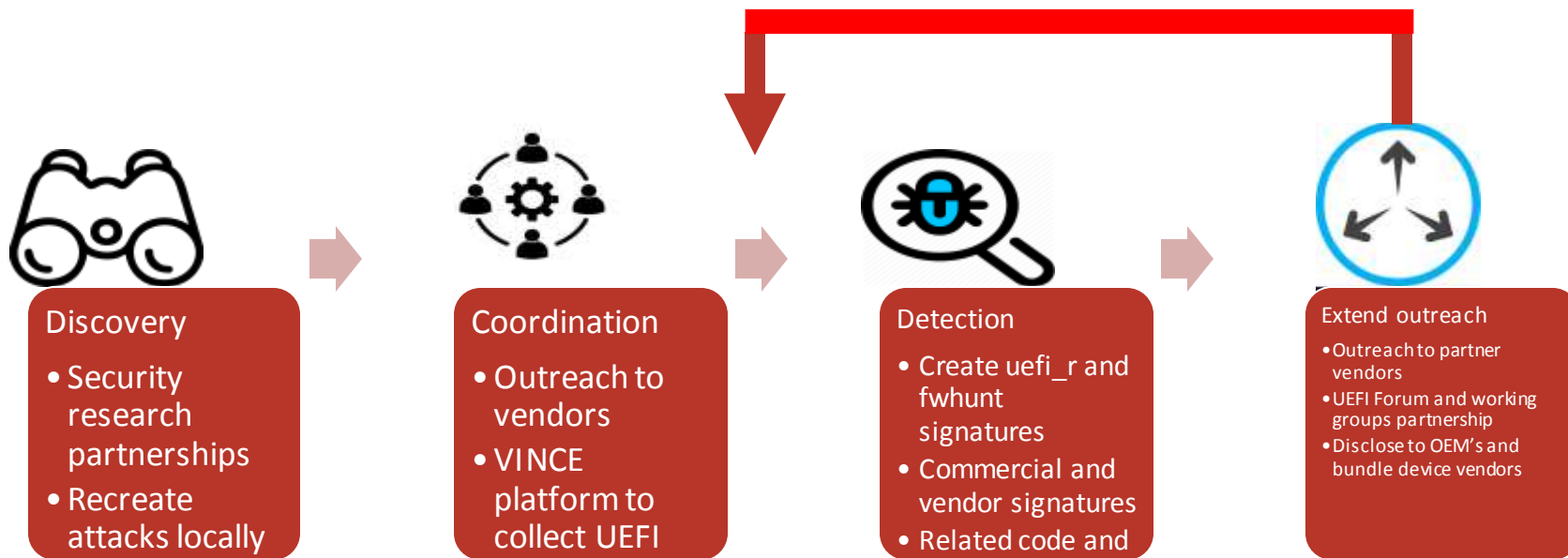


UEFI phases of danger – even AfterLife is not safe



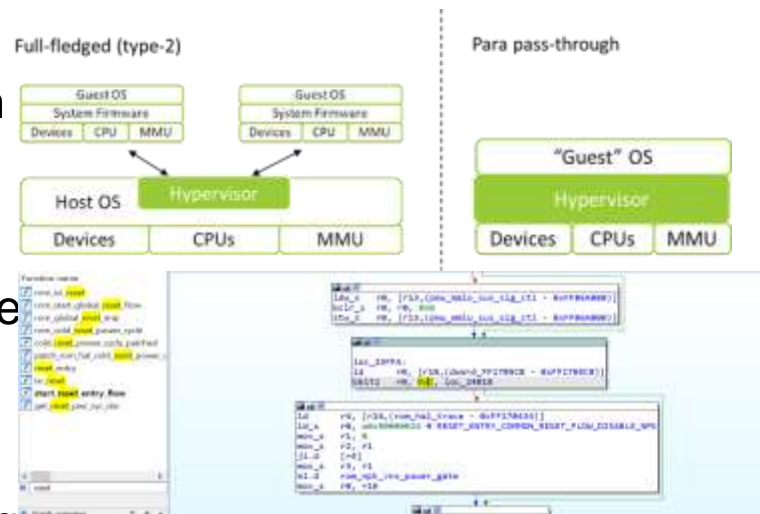
UEFI boot phases as described in EDK2 do not have a reference code/implementation has many vulnerabilities managed by many vendors

Desired approach for UEFI vulnerability lifecycle

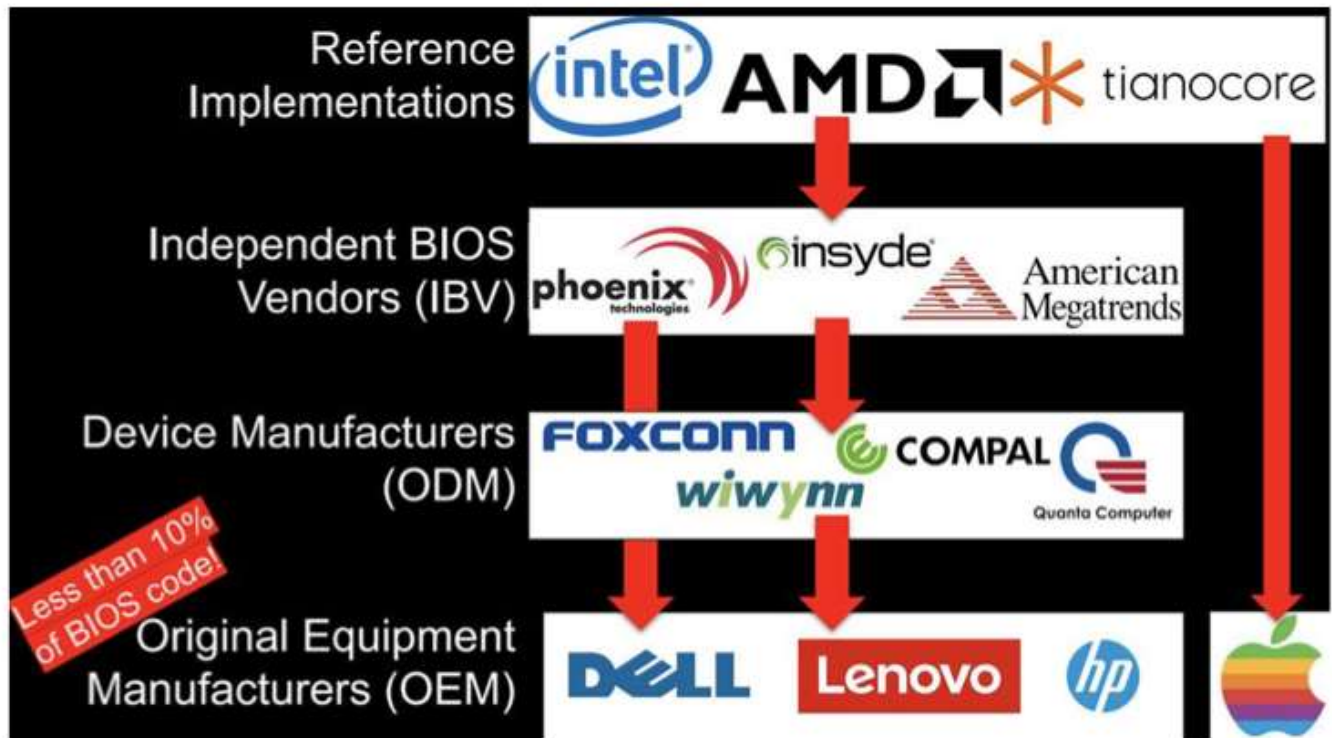


Vulnerability discovery approaches and key players as partners

- Binary analysis and UEFI SMM attacks n
 - Binary Extended Threat modeling – A
 - Eclipsium focused on bootkits/rootkits
- Attacking Virtualization and peripherals
 - CrowdStrike focused on Virtualization
 - Tanda
 - Google Project Zero – Diane Dubois
- Attacking microcode and PCH hardware
 - Gorychev and Mark Ermolov
- Intel ME attacks modeling
 - Looking for partners (iStare Intel bought them)



Coordination - the Supply Chain players – reference names



[Image courtesy Alex Matrosov Binary](#)

UEFI Capsule updates and LVFS repository

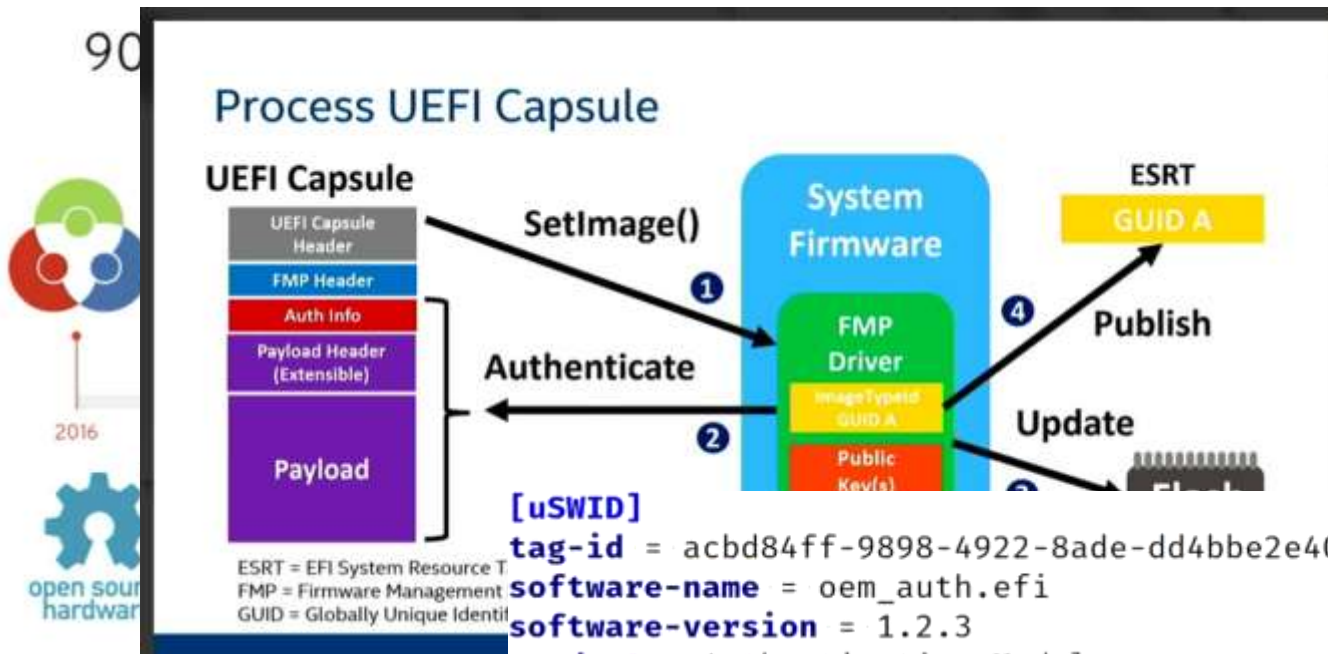


Image from [Richard Hughes](#)

[uSWID]

tag-id = acbd84ff-9898-4922-8ade-dd4bbe2e40ba

software-name = oem_auth.efi

software-version = 1.2.3

product = Authentication Module

summary = Hughski Super-Secret-Sauce Authentication Module

colloquial-version = b2ed6f1ed8587bf01a2951d74512a70f1a512d38



revision = 2

Currently only fw hunt rules are open source. We are looking for more help and partnership – Eclipsium, CrowdStrike potential researchers

Collecting, tagging and maintaining UEFI capsules in MASS

Results:

8,855 hits for tag 'lvfs' in the MASS

	0255bca937b1897281b1d9d8bab5e233 First seen on Thu, 10 Mar 2022 21:43:58 GMT ** File type: archive/mscab	lvfs firmware fwupdate
	036fe9dfe9151a0884f1b0ed695880eb First seen on Wed, 18 May 2022 17:18:03 GMT ** File type: archive/mscab	lvfs fwupdate
	05c45b55c9be73d9894bf26c93b9dbf2 First seen on Thu, 10 Mar 2022 21:42:07 GMT ** File type: archive/mscab	lvfs cve-2021-39301 cve-2021-39299 cve-2021-39297 fwupdate firmware cve-2021-39300
	0a47410a437ce377a499cc85ac7b6f08 First seen on Thu, 10 Mar 2022 18:46:53 GMT ** File type: archive/mscab	lvfs firmware fwupdate
	1288ae8d6fdb12708ff764339979e01b First seen on Thu, 10 Mar 2022 21:46:02 GMT ** File type: archive/mscab	lvfs firmware fwupdate
	2776fca4fa3176ca046a753cef32f0cc First seen on Thu, 10 Mar 2022 21:44:07 GMT ** File type: archive/mscab	lvfs firmware fwupdate
	2ee806ef1a8a2ddbfc4e747148d708df First seen on Thu, 10 Mar 2022 21:41:41 GMT ** File type: archive/mscab	lvfs firmware fwupdate

UEFI vulnerabilities all flavors now in VINCE

UEFI Vulnerability types and methods are growing

VU#434994: TOCTOU Race Conditions in UEFI Vulnerability OS and Firmware DMA Timing Active CERT/CC

Last updated 2022-05-18 (3 hours ago)

VU#796611: InsydeH2O UEFI BIOS impacted by multiple vulnerabilities Active Published CERT/CC

Last updated 2022-04-26 (3 weeks, 1 day ago)

VU#917518: HP UEFI System Firmware (S74

Last updated 2022-03-23 (1 month, 3 weeks ago)

VU#583814: Multiple memory corruption v

Last updated 2022-03-08 (2 months, 1 week ago)

VU#109929: Insyde UEFI software on Edge

Last updated 2022-03-02 (2 months, 2 weeks ago)

VU#174059: GRUB2 boot loader is vulnerat

Last updated 2020-08-25 (1 year, 8 months ago)

VU#766164: Intel BIOS locking mechanism

Last updated 2020-05-22 (1 year, 12 months ago)

VU#552286: UEFI EDK2 Capsule Update vul

Last updated 2020-05-22 (1 year, 12 months ago)

VU#507496: GIGABYTE BRIX UEFI firmware

Last updated 2020-05-22 (1 year, 12 months ago)

VU#533140: Tianocore UEFI implementatio

Last updated 2020-05-22 (1 year, 12 months ago)

VU#316011: Malicious UEFI Bios Firmware

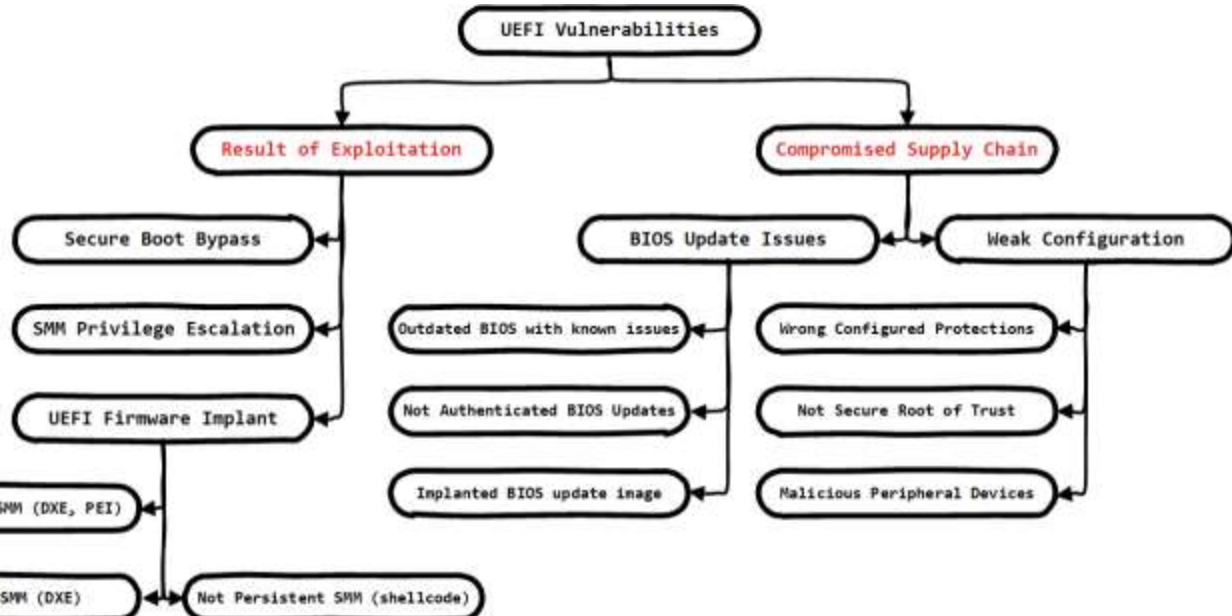
Last updated 2020-05-22 (1 year, 12 months ago)

VU#354550: Vulnerability in UEFI Capsule U

Last updated 2020-05-22 (1 year, 12 months ago)

VU#329192: UEFI contains a shell vulnerability that allows a modified microupdate file to load upon bootup of all uefi systems

Active



FwHunt detection and analysis of vulnerable capsules.



Richard Hughes
Coordinator
Principal Engineer

2021-12-10 (5 months, 1 week ago)

Affected machines on the LVFS:

- Lenovo ThinkPad L13
- Lenovo ThinkPad L14 Gen 1 / L15 Gen 1
- Lenovo ThinkPad L14 Gen 2 / L15 Gen 2
- Lenovo ThinkPad P1 Gen 3/X1 Extreme 3rd
- Lenovo ThinkPad P1 Gen 4/X1 Extreme Gen 4
- Lenovo ThinkPad P15 Gen 1/ P17 Gen 1/ P15g Gen 1/ T15p Gen 1/ P15v Gen 1
- Lenovo ThinkPad P15 Gen 2/ P17 Gen 2/ T15g Gen 2
- Lenovo ThinkPad T14 Gen 1/ P14s Gen 1 / T15 Gen 1 / P15s Gen 1 / T14 Gen 1 Healthcare Edition
- Lenovo ThinkPad T14 Gen 2 / P14s Gen 2 / T15 Gen 2 / P15s Gen 2
- Lenovo ThinkPad T14s Gen 1 / ThinkPad X13 Gen 1
- Lenovo ThinkPad T14s Gen 2 / X13 Gen 2
- Lenovo ThinkPad T490
- Lenovo ThinkPad X1 Carbon 7th / X1 Yoga 4th
- Lenovo ThinkPad X1 Carbon 9th / X1 Yoga 6th
- Lenovo ThinkPad X1 Carbon Gen 8 /X1 Yoga Gen 5
- Lenovo ThinkPad X13YogaGen1
- Lenovo ThinkPad X13YogaGen2
- Lenovo ThinkPad X390
- Lenovo ThinkStation M70A
- Star Labs StarBook MkV

Intel NUC laptop is vulnerable to SMM memory corruption

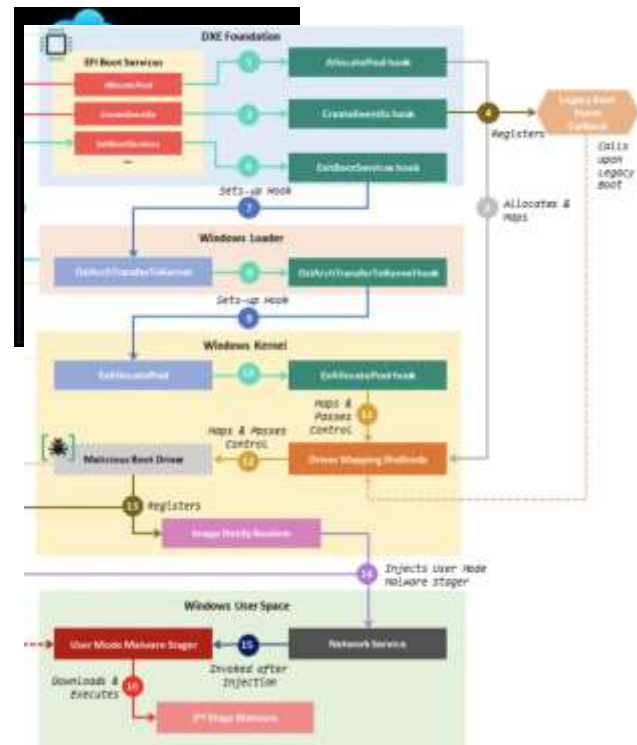
Reported by Alex Matrosov – September 2021
Denied by Intel and unacknowledged by vendors – October 2021

Richard Hughes scans using fwhunt – Found 20 models of Lenovo, StarLabs impacted
About 40 vendors have the code
Unknown number of models impacted that is outside of LVFS.

Reply

Forward looking research areas and security concerns

- Microsoft Pluton will make it difficult to write implants and self-updating malware. Persistence will become most difficult.
- Chip-to-Cloud approach expected from all vendors like HPE, Lenovo, Dell, Apple and some chip vendors AMD.
- Intel ME and AMD PSP expected to give more capability to access hardware and even in some cases overwrite microcode.
- Attackers have to look at other places for persistence
- Moonbounce is the latest one in the news, but MosaicRegressor, BootHole are early but less sophisticated.



Ongoing work and next steps

- Continue our own exploit research for discovering vulnerabilities and reproducing attacks against UEFI. Enhance work such as parsers, code detection techniques specifically for UEFI.
- Extend partnership with some large researchers and vendors to highlight UEFI security concerns – Sentinel, Intel iStare division.
- Bring more transparency into the UEFI ecosystem - addition of SBOM coSWID, automated detection of reuse of code, fingerprinting and auditing of valid UEFI code (inside capsules).
- Outreach to UEFI Forum about creating a security working group and look into ways to bring transparency.
- Explore other projects like Coreboot and Libreboot bringing transparency and reducing –ve Rings in Protection Ring of modern OS (less likely).

Engage with Us



Download [software and tools](#)

Participate in [education](#) offerings

Attend an [event](#)

Search the [digital library](#)

Read the [SEI Year in Review](#)

Explore our [research and capabilities](#)

[Collaborate](#) with the SEI on a new project

Contact Us



Carnegie Mellon University
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213
888-201-4479

info@sei.cmu.edu
www.sei.cmu.edu