presented by

Coordinating UEFI Vulnerabilities as CERT/CC

UEFI 2024 Virtual Plugfest

November 21, 2024

Vijay Sarvepalli

License Information and Markings

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.

[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 was prepared for the exclusive use of Mitre and CVE Working Group. and may not be used for any other purpose without the written consent of permission@sei.cmu.edu.

DM24-1338

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution

Meet the Presenter

Vijay Sarvepalli

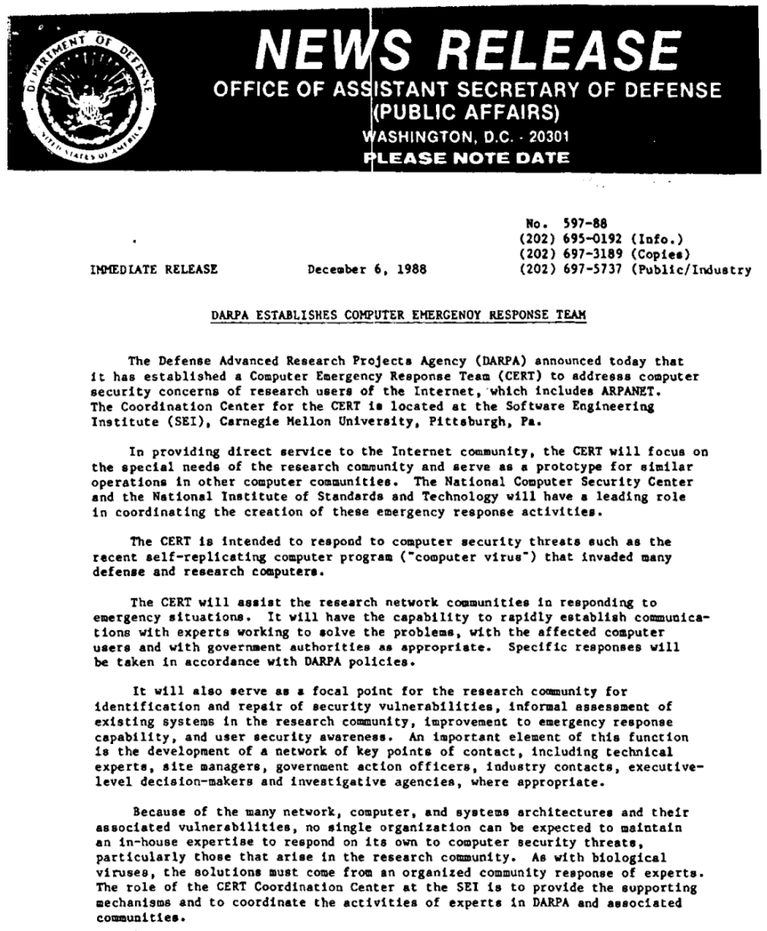
Principal Architect,
CERT Threat Analysis SEI of Carnegie Mellon University

28 years of experience in various large-scale software systems with recent 15 years in software security with specific focus on Vulnerability Management and Threat Analysis

Agenda

- CERT/CC Introduction
- Vulnerability Coordination Roles
- Systemic Vulnerability Focus and UEFI
- UEFI Vulnerability Challenges
- Collaboration and Call-to-Action
- Q & A

CERT/CC - The Beginnings…



NEWS RELEASE
OFFICE OF ASSISTANT SECRETARY OF DEFENSE
(PUBLIC AFFAIRS)
WASHINGTON, D.C. 20301
PLEASE NOTE DATE

No. 597-88
(202) 695-0192 (Info.)
(202) 697-3189 (Copies)
(202) 697-5737 (Public/Industry

IMMEDIATE RELEASE December 6, 1988

DARPA ESTABLISHES COMPUTER EMERGENOY RESPONSE TEAM

The Defense Advanced Research Projects Agency (DARPA) announced today that it has established a Computer Emergency Response Team (CERT) to addresss computer security concerns of research users of the Internet, which includes ARPANET. The Coordination Center for the CERT is located at the Software Engineering Institute (SEI), Carnegie Mellon University, Pittsburgh, Pa.

In providing direct service to the Internet community, the CERT will focus on the special needs of the research community and serve as a prototype for similar operations in other computer communities. The National Computer Security Center and the National Institute of Standards and Technology will have a leading role in coordinating the creation of these emergency response activities.

The CERT is intended to respond to computer security threats such as the recent self-replicating computer program ("computer virus") that invaded many defense and research computers.

The CERT will assist the research network communities in responding to emergency situations. It will have the capability to rapidly establish communications with experts working to solve the problems, with the affected computer users and with government authorities as appropriate. Specific responses will be taken in accordance with DARPA policies.

It will also serve as a focal point for the research community for identification and repair of security vulnerabilities, informal assessment of existing systems in the research community, improvement to emergency response capability, and user security awareness. An important element of this function is the development of a network of key points of contact, including technical experts, site managers, government action officers, industry contacts, executive-level decision-makers and investigative agencies, where appropriate.

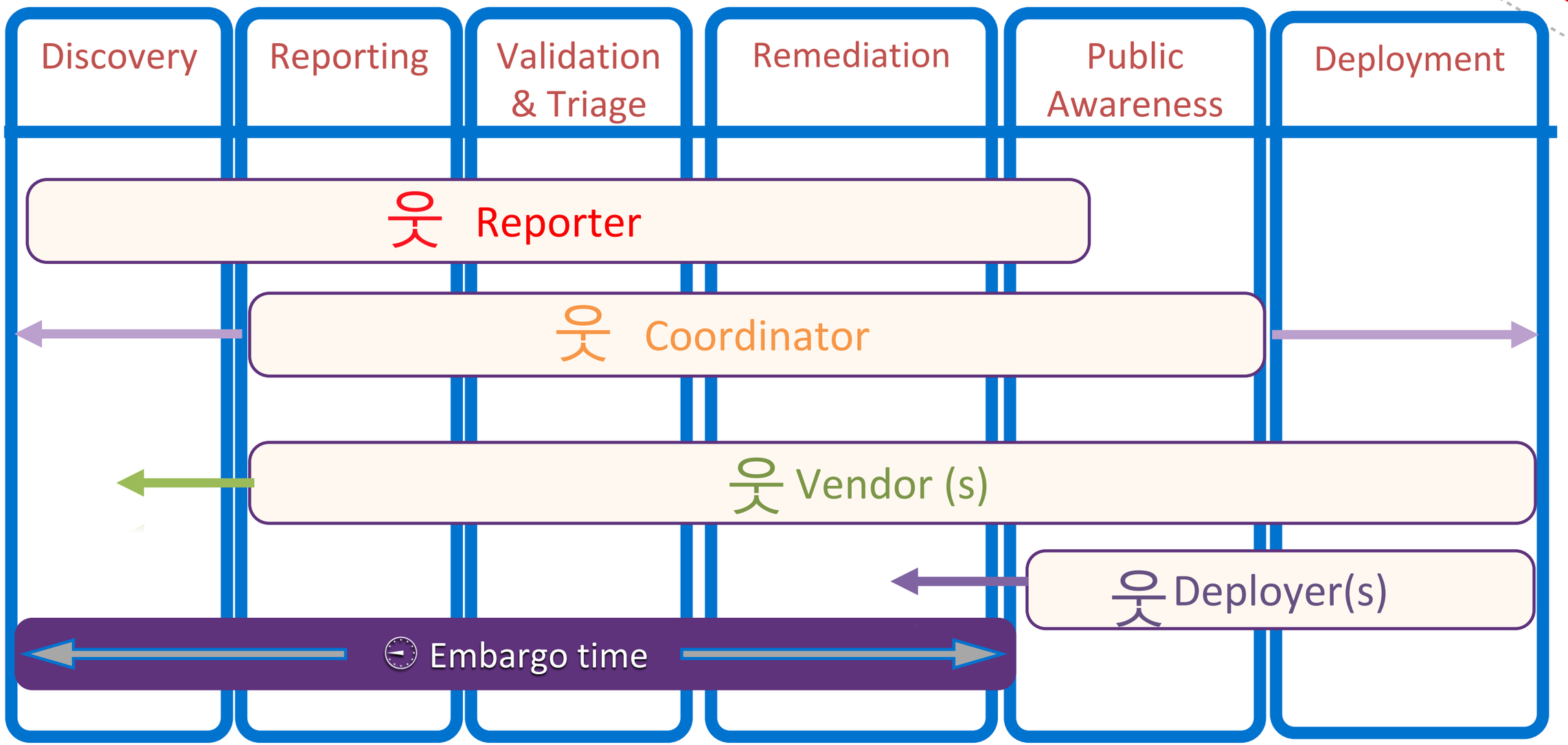
Because of the many network, computer, and systems architectures and their associated vulnerabilities, no single organization can be expected to maintain an in-house expertise to respond on its own to computer security threats, particularly those that arise in the research community. As with biological viruses, the solutions must come from an organized community response of experts. The role of the CERT Coordination Center at the SEI is to provide the supporting mechanisms and to coordinate the activities of experts in DARPA and associated communities.

- The Software Engineering Institute is a non-profit United States federally funded research and development center, where CERT Coordination Center (CERT/CC) is the coordination center of the computer emergency response team
- The first organization of its kind, the SEI's CERT/CC was created in Pittsburgh in November 1988 at DARPA's direction in response to the Morris worm incident

Vulnerability Coordination Roles

- From Incidents to Vulnerability Coordination to reach Vendors and Product sources of vulnerability
- CERT/CC formulates and adopts Coordinated Vulnerability Disclosure (CVD) guide to help collaborative way between Reporters and Vendors to resolve software security
- CERT/CC depends on discovery of vulnerability done by independent researchers and research organizations (including ourselves)
- CERT/CC is funded by the US Government - recent specific focus on Systemic Vulnerabilities and Supply-Chain concerns.
- CERT/CC can play an active roles in multi-vendor coordination acting as a clearing house to reach US Government EO 14028

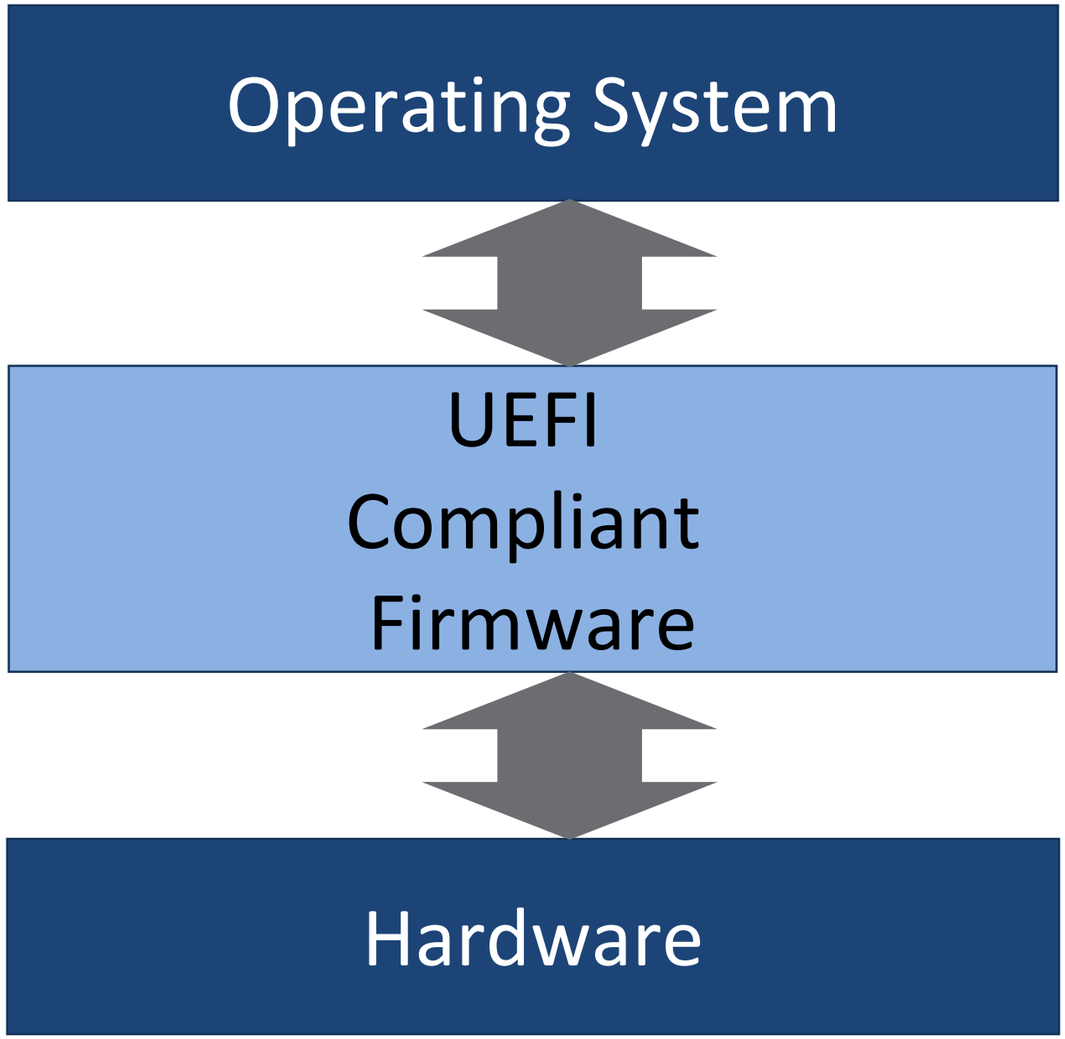
Typical Coordination Workflow



What is a Vulnerability, Systemic Vulnerability?

- What is a Vulnerability?
  - NIST 800-28 - A flaw or weakness in a computer system, its security procedures, internal controls, or design and implementation, which could be exploited to violate either explicit or implicit security policy
- What is a Systemic Vulnerability?
  - A systemic vulnerability is a deeply embedded flaw that is pervasive across multiple systems, vendors, or implementations, challenging to detect and remediate due to complex dependencies, elusive root causes, and often dismissed as inherent to the system, making it highly resistant to effective remediation and prone to recurrence

Introducing 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 provides:

- Faster boot times (Speed)
- Wider range of device support (Interoperability)
- Catchup with Moore's law (Growth)
- User-Friendly Interface (HCI)

Is UEFI a Systemic Vulnerability Area?

- An attempt to narrow down Systemic Vulnerability brings us two threat related focus areas
  - Persistence “pursues its objectives repeatedly over an extended period of time”
  - Invisibility “currently invisible to OS/Security software for audits/quality/pedigree”
- In September 2020, our Threat Team finds an attack labeled MIDNIGHT that uses UEFI Environment for persistence; OS, EDR cannot detect
- In later 2020, we launch of our focus area for understanding and mitigating UEFI Vulnerabilities

Is UEFI a Systemic Vulnerability Area?

- UEFI software is built with many components - a supply-chain challenge and remains invisible to many OS and Security software
- UEFI vulnerabilities are difficult to explain, UEFI Vendors have limited security outreach and limited ability to trickle down supply-chain
- CERT/CC initiates outreach to Security Researchers, Vendors, OEMs that are involved in UEFI
- Sample UEFI Vulnerability Case handling took many months (sample EDK2 14 months), and some implementations remained unresolved

Can UEFI be Attacked? Threats?

- Attacks against UEFI continues to evolve
- Complex variants chain vulnerabilities
- Persistence and Invisibility both possible
- Threat groups want to target Intel ME using UEFI
- Attacks against UEFI software suppliers

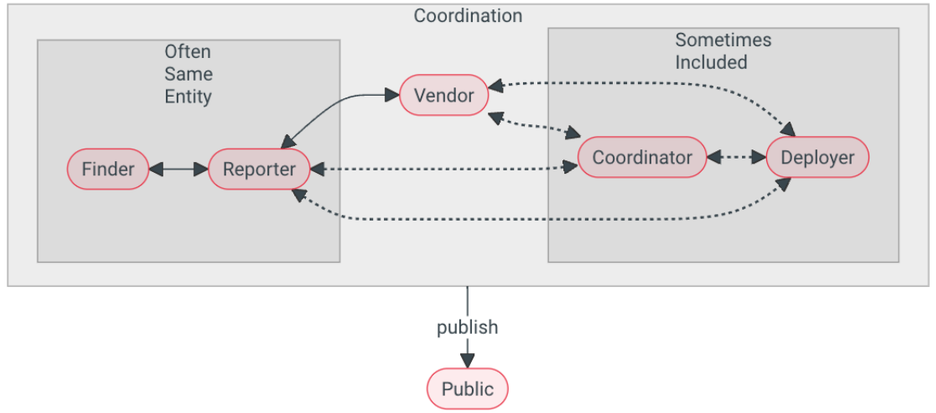
UEFI Vulnerability Unique Challenges

- Vulnerability reporting is difficult due to lack of understanding and complexity
- Every UEFI vulnerability can be considered a supply-chain vulnerability - reuse, repurposed, outsourced, bundled are common phenomena
- Hard to patch- Firmware storage limited in PCI Flash sometimes encrypted, inaccessible and patching may require multiple reboots
- Difficult to verify patches and current version of patched firmware
- Outreach from open-source components not established or reliable.
- Potential private coordination and no CVE, no public advisory, transparency

Image from UEFI.ORG Presentation 2023

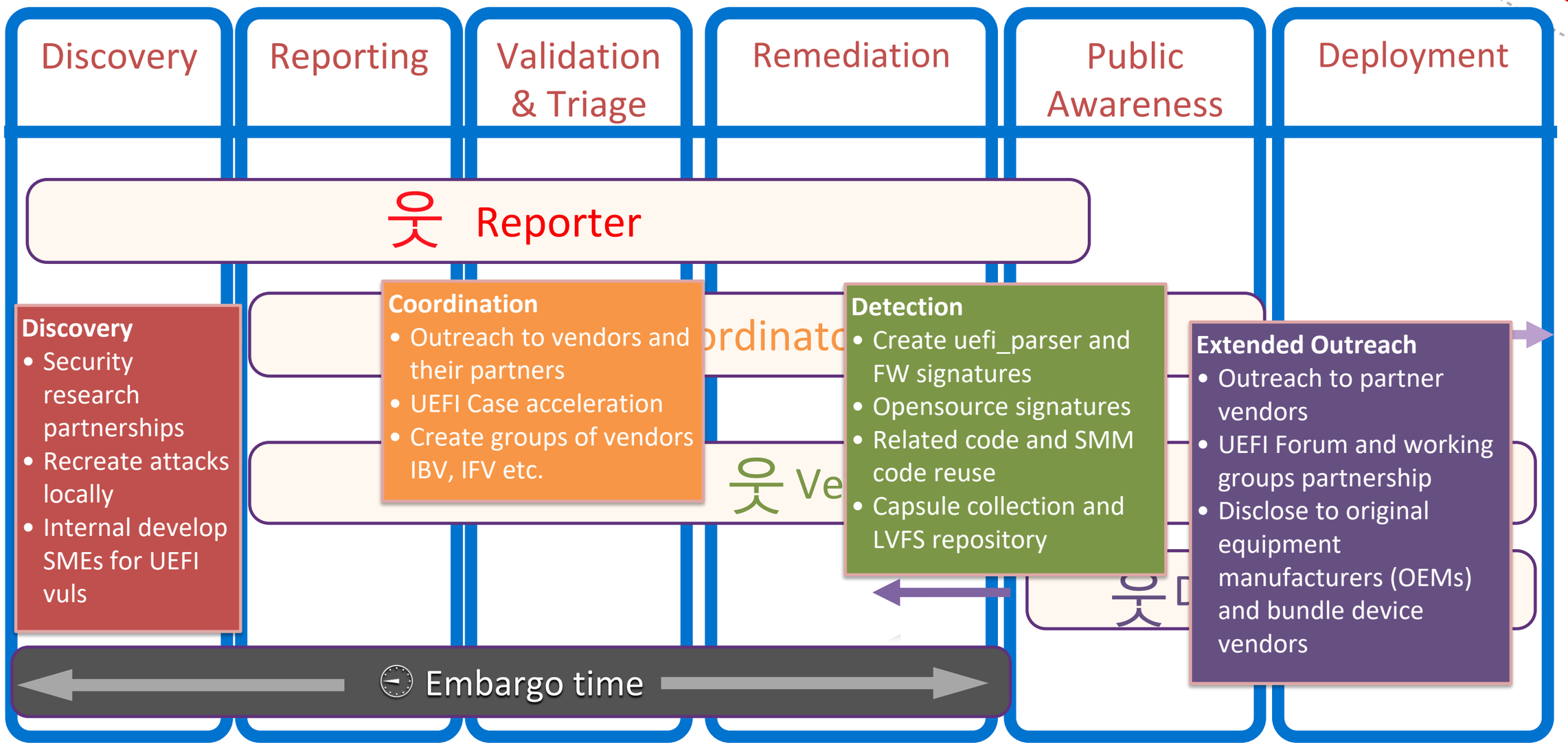
CVD Multi-Party Approach Can Help

- CVD viable and reliable process for timely Vulnerability Response
- Active participation in CERT/CC multi-vendor and international partners can provide an open outreach
- Private outreach to Researchers and other Vendors possible
- Opensource community outreach is possible



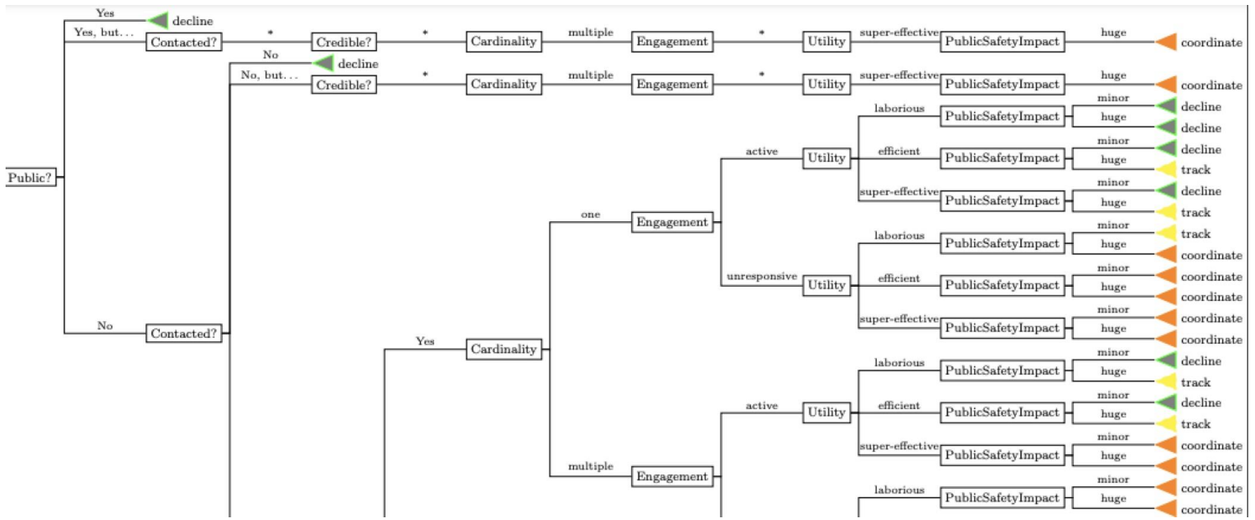
https://certcc.github.io/CERT-Guide-to-CVD/

UEFI Coordination Workflow



CERT/CC CVD Working with You

- CVD work is initiated by a security researcher submitting a vulnerability report to our site https://kb.cert.org
- We triage our vulnerability coordination using SSVC to prioritize. Exceptions: Systemic Vulnerability, undocumented yet exploited vulnerability, “zero-day”
- Reports are collected with as much relevant information to connect Researcher to Vendor(s)
- We manage Vendor contacts with public information and self-management tools for Vendors



[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution

UEFI Vulnerability Handled by CERT/CC

VU#132380: Vulnerabilities in EDK2 NetworkPkg IP stack implementation. Active Published uefi CERT/CC
Last updated 2024-10-09 (1 week, 5 days ago)

VU#455367: Insecure Platform Key (PK) used in UEFI system firmware signature Active Published uefi CERT/CC
Last updated 2024-08-30 (1 month, 3 weeks ago)

VU#109929: Insyde UEFI software on Edge server environments impacted by vulnerabilities Active uefi CERT/CC
Last updated 2024-08-05 (2 months, 2 weeks ago)

VU#917518: HP UEFI System Firmware (S74) vulnerable to buffer overflow Active uefi CERT/CC
Last updated 2024-08-05 (2 months, 2 weeks ago)

VU#434994: TOCTOU Race Conditions in UEFI Vulnerability OS and Firmware DMA Timing Active Published uefi CERT/CC
Last updated 2024-08-05 (2 months, 2 weeks ago)

VU#504718: Multiple vulnerabilities disclosed in the signed UEFI bootloader shim Active uefi CERT/CC
Last updated 2024-07-29 (2 months, 3 weeks ago)

VU#275256: Vulnerabilities in EDK2 Reference implementation of the UEFI Specification Inactive uefi CERT/CC
Last updated 2024-06-12 (4 months, 1 week ago)

VU#158026: AMI APTIO V UEFI firmware is vulnerable to privilege escalation during Pre-EFI Initialization phase. Inactive uefi CERT/CC
Last updated 2024-06-11 (4 months, 1 week ago)

VU#892082: Tiancore EDK2 UEFI TCG2 reference implementation vulnerable to memory corruption Inactive uefi CERT/CC
Last updated 2024-06-11 (4 months, 1 week ago)

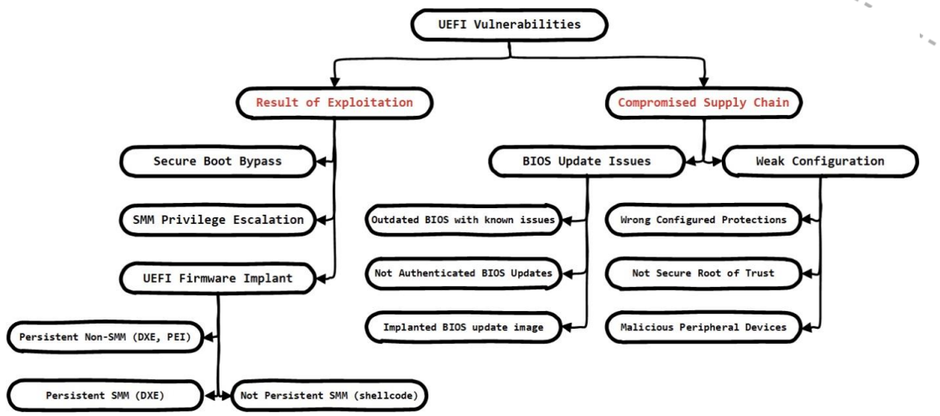
VU#796611: InsydeH2O UEFI BIOS impacted by multiple vulnerabilities Inactive Published uefi CERT/CC
Last updated 2024-06-11 (4 months, 1 week ago)

VU#527547: Samsung Galaxy Pro laptops UEFI implementation vulnerable to SMM memory corruption Inactive uefi CERT/CC
Last updated 2024-06-11 (4 months, 1 week ago)

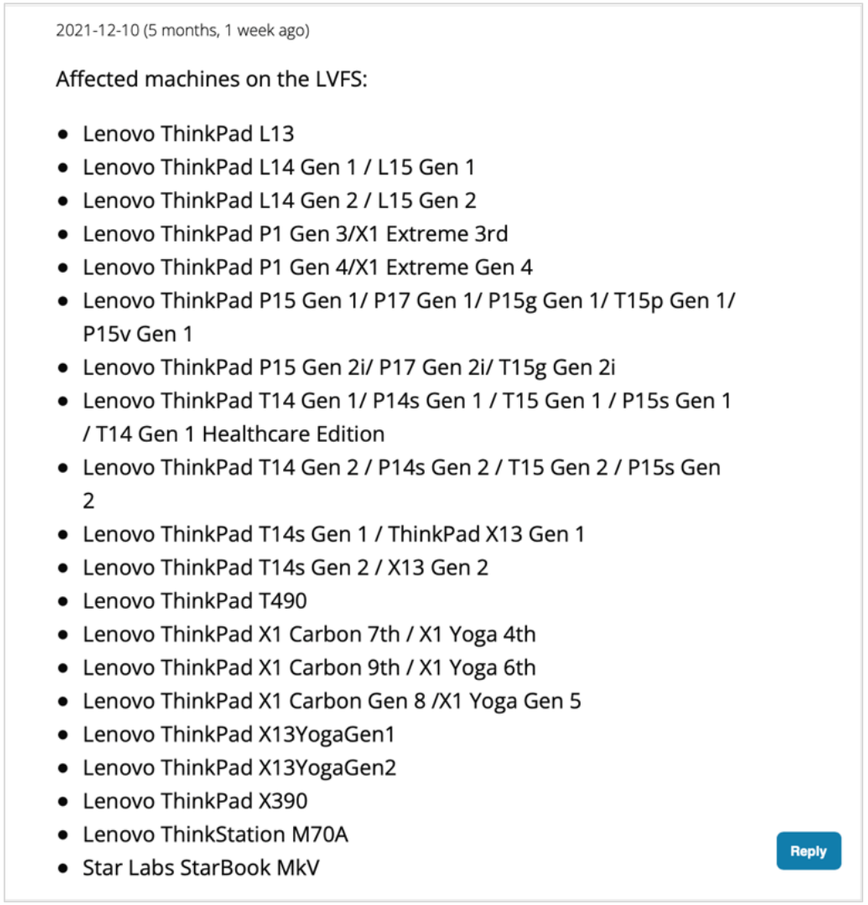
VU#683814: Multiple memory corruption vulnerabilities in HP UEFI SMM (System Management Mode) engine Inactive uefi CERT/CC
Last updated 2024-06-11 (4 months, 1 week ago)

VU#309662: These 3 Microsoft signed bootloaders allow to bypass secure boot Inactive Published uefi CERT/CC
Last updated 2024-04-17 (6 months ago)

VU#801185: Signed UEFI Shell binary by GeTac can be abused to get untethered access to UEFI memory Active uefi CERT/CC
Last updated 2024-03-11 (7 months, 1 week ago)



UEFI Supply-Chain is Complex



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 2i/ P17 Gen 2i/ T15g Gen 2i
- 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

Reply

The Intel NUC laptop is vulnerable to SMM memory corruption:

- Reported in September 2021 to Intel
- Intel considered this vulnerability in a product with “End of Servicing Updates” or unsupported and unacknowledged by vendors —October 2021
- Opensource scans using FW signatures found 20 models of Lenovo; StarLabs impacted.
- About 40 vendors have the code.
- There are unknown number of models impacted that are outside of LVFS.
- Reuse of code is prevalent but vendors are unaware of it.

Coordinator's Dilemma & UEFI Vendors

- Researcher and Vendor are in crossroads about Vulnerability - timing, details, credits, oh my…
- In multi-vendor case, most Vendors like to consume but never corroborate or collaborate for coordination
- Vendors confused about Disclosure purpose - a public statement, competitive edge/exclusion, "Affected" or "Not Affected" disputes, liability, financial disadvantage
- Researchers confused of Disclosure purpose - an amplifying social media voice, providing value for their product/service, valuable research output.

CERT/CC Coordination Principles

- Every advisory is measured back against purpose - public awareness and public welfare
- Reduce confusion, duplication and ambiguity
- Expect distributed way of information gain instead of central authoritative source
- Assume that all parties work in honesty, good faith and benevolence

Call for UEFI Collaboration

- All UEFI software providers should consider security point of contact and security vulnerability reporting workflow - PSIRT consider CISA pledge
- All UEFI digital signing should include a PSIRT contact for tracking and response. Potentially a certificate extended attribute
- UEFI Forum members can ensure their partners and their suppliers have support for vulnerability reporting workflow or augment support
- PSIRT should provide simple ways to reach like securirty@example.com and .well-known/security outreach methods
- Vulnerability Management does beyond SDLC and deployment - it is response to a vulnerability trigger

UEFI Security is…

- **Critical:** UEFI Security is critical to prevent attacker's foothold that is persistent and invisible
- **For Everyone:** Security goes beyond interoperability and reliability - consider CIA
- **Requires Outreach**: Collaboration outside your downstream, upstream suppliers is crucial for security
- **Establishes Trust boundaries:** begins close to the bottom of chip-to-cloud today's architecture
- **Protect National and Global Interests:** CISRTs, CERTs, CSIRTS and other organizations are keenly dependent on it

UEFI Security is…

- CERT/CC VINCE Portal - https://kb.cert.org/vince/
- CERT/CC Advisory Database - https://kb.cert.org/
- A better metric SSVC https://certcc.github.io/SSVC/
- CISA Vulnrichment - https://github.com/cisagov/vulnrichment
- CISA Pledge - https://www.cisa.gov/securebydesign/pledge

Questions?

More Questions?

Following today's webinar, join the live, interactive Microsoft Teams Q&A for the opportunity to chat with the presenters

Visit this link to attend: https://bit.ly/4flj00g

Meeting ID: 215 180 381 97

Password: DnKMue

Thanks for attending a UEFI Forum sponsored webinar

For more information on UEFI Forum and UEFI Specifications, visit http://www.uefi.org

presented by