Hardware CWE™ Special Interest Group (SIG)

Gananand Kini, Bob Heinemann, Luke Malinowski, Gage Hackford, Chris Lathrop, Steve Christey Coley, Alec Summers

MITRE

August 18, 2023

Agenda

REMINDER: This meeting is being recorded.

- **Housekeeping and Announcements**
- **Working Items for this meeting:**

1	CWE Nit Bits	Bob H	5 min
2	Discussion: Covert Channels and CWE	Bob H	10 min
3	Discussion: Most Important Hardware Weaknesses Refresh	Bob H	10 min
4	AOB (Any Other Business)		

Housekeeping

- **Schedule:**
  - **Next Meeting:**
    - **September 8th**
    - **12:30 – 1:30 PM EST (16:30 – 17:30 UTC)**
    - **Microsoft Teams**
- **Contact: cwe@mitre.org**
- **Mailing List:** *hw-cwe-special-interest-group-sig-list@mitre.org*
- **Minutes from previous meetings available on our GitHub site:**
  - **https://github.com/CWE-CAPEC/hw-cwe-sig**

Announcements

- **Tentative: CISA strategy around Secure By Design/Secure By Default for Sep SIG**

CWE Nit Bits

B*ite-sized knowledge*
that will enhance your CWE proficiency!

Vulnerability Mapping Notes

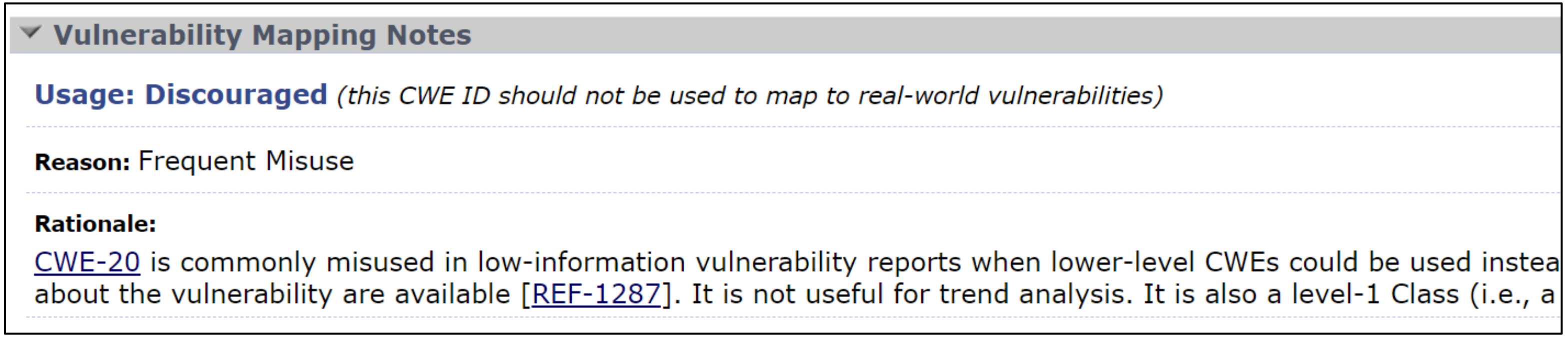
Provides guidance for when or whether to map an issue to a particular CWE entry or to suggest alternatives.

- **Usage:** describes whether the CWE should be used for mapping vulnerabilities to their underlying weaknesses as part of root cause analysis.
- **Reason:** uses a limited vocabulary to summarize the Usage.
  - Allowed, Allowed-with-Review, Discouraged, etc.
- **Rationale:** provides context for the Usage.
- **Comments:** provides further clarification to the reader.
- **Suggestions:** includes suggestions for additional CWEs that might be more appropriate for the mapping task.

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

Examples

CWE-20: Improper Input Validation



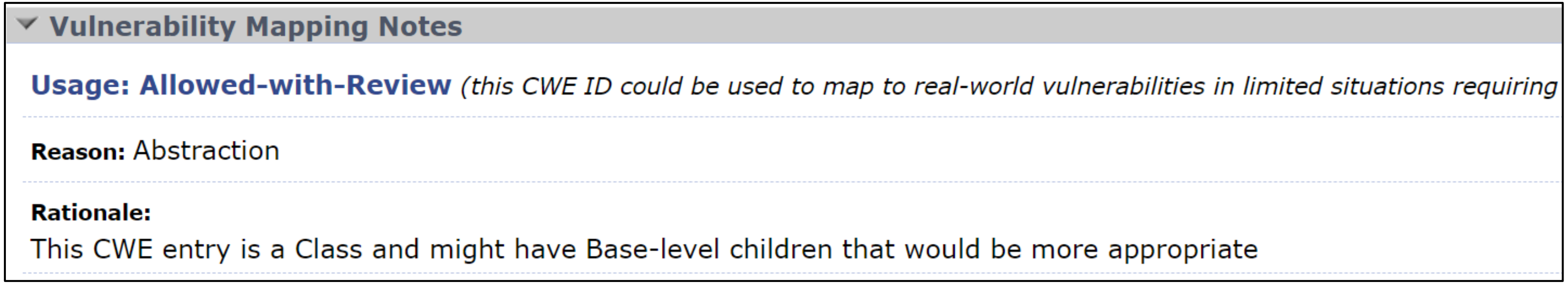
Vulnerability Mapping Notes

Usage: Discouraged *(this CWE ID should not be used to map to real-world vulnerabilities)*

Reason: Frequent Misuse

Rationale:
CWE-20 is commonly misused in low-information vulnerability reports when lower-level CWEs could be used instea
about the vulnerability are available [REF-1287]. It is not useful for trend analysis. It is also a level-1 Class (i.e., a

CWE-514: Covert Channel



Vulnerability Mapping Notes

Usage: Allowed-with-Review *(this CWE ID could be used to map to real-world vulnerabilities in limited situations requiring*

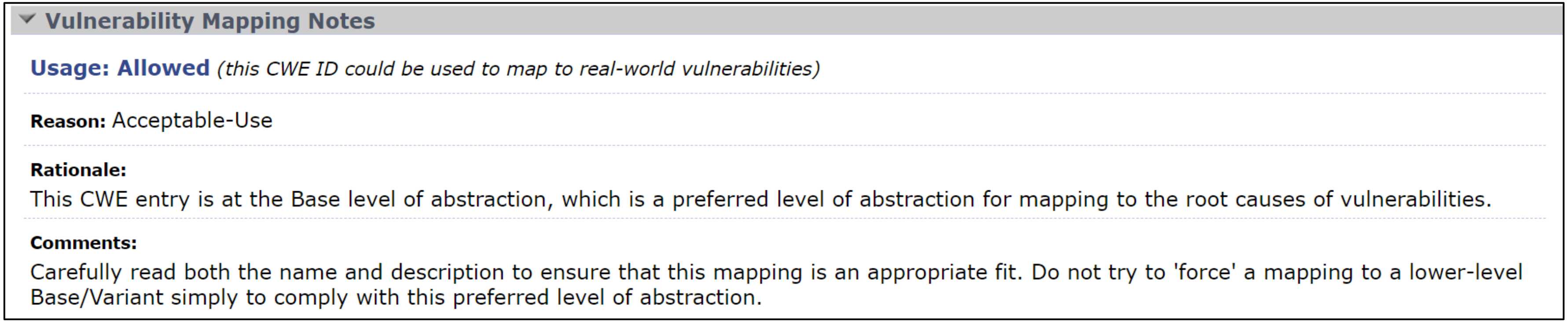
Reason: Abstraction

Rationale:
This CWE entry is a Class and might have Base-level children that would be more appropriate

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

Example 2

CWE-1277: Firmware Not Updateable



Vulnerability Mapping Notes

Usage: Allowed *(this CWE ID could be used to map to real-world vulnerabilities)*

Reason: Acceptable-Use

Rationale:

This CWE entry is at the Base level of abstraction, which is a preferred level of abstraction for mapping to the root causes of vulnerabilities.

Comments:

Carefully read both the name and description to ensure that this mapping is an appropriate fit. Do not try to 'force' a mapping to a lower-level Base/Variant simply to comply with this preferred level of abstraction.

Covert Channel Coverage in CWE

COVID-Bit Research Item[1][2]

- **In 2022, researchers at Ben Gurion University in Israel developed a new data exfiltration method for air-gapped systems called COVID-bit.**
- **Malware generates electromagnetic radiation in the 0-60 kHz frequency band (assumes Malware got there somehow).**
- **EM emissions are generated by manipulating the workload of the CPU. Claims of indirect control SMPS.**
- **The electromagnetic radiation generated by this intentional process can be received from a distance using appropriate antennas.**

1. *https://thehackernews.com/2022/12/covid-bit-new-covert-channel-to.html?m=1*
2. *https://arxiv.org/abs/2212.03520*

Covert Channels and Side Channels

- Initial thought was that COVID-Bit could be a DEMOX for CWE-1300: Improper Protection of Physical Side Channels
- As HW SIG Members had correctly pointed out, COVID-Bit is about Covert Channels and NOT Side Channels
- Covert Channel (CC) / Side Channel (SC)
  - Intentional transmission (CC). Accidental transmission (SC) – *Ross Anderson* [1]
  - Adversary controls input and output (CC). Adversary can only read output (SC) – *Intel* [2]
  - Not an intended resource but exists due the application's behaviors. –*CWE-514 Notes* [3]
- If not CWE-1300 (SC), where would something like this map to in HW view?
- Closest we have is CWE-514: Covert Channels

1. *https://www.cl.cam.ac.uk/~rja14/Papers/SEv3-ch19-7sep.pdf*
2. *https://www.intel.com/content/www/us/en/developer/articles/technical/software-security-guidance/best-practices/refined-speculative-execution-terminology.html*
3. *https://cwe.mitre.org/data/definitions/514.html*

CWE-514: Covert Channel

https://cwe.mitre.org/data/definitions/514.html

Abstraction: Class

Description: A covert channel is a path that can be used to transfer information in a way not intended by the system's designers.

Extended Description: Typically the system has not given authorization for the transmission and has no knowledge of its occurrence.

Relationships:

ChildOf	CWE-1229:Creation of Emergent Resource
ParentOf	CWE-385:Covert Timing Channel
ParentOf	CWE-515: Covert Storage Channel
CanFollow	CWE-205: Observable Behavioral Discrepancy

Vulnerability Mapping Notes:

Usage: Allowed-with-Review; **Reason:** Abstraction

Rationale: This CWE entry is a Class and might have Base-level children that would be more appropriate; **Comments:** Examine children of this entry to see if there is a better fit.

NOTE: Nothing about EM based Covert Channels, nor HW cause, e.g., SMPS

Discussion

Questions:

- Should we place CWE-514 in the HW View?
- Do we need to modify CWE-514 to be less software centric?
- Or create a base of CWE-514 and put that into the HW view?

Previous HW SIG Member Comments:

- Covert Channels should have coverage in the hardware view *–Jason Oberg*
- Covert Channels should be in the HW categories Security Flow Issues, General Circuit and Logic Design Concerns, or Debug and Test Problems. *–Paul Wortman*

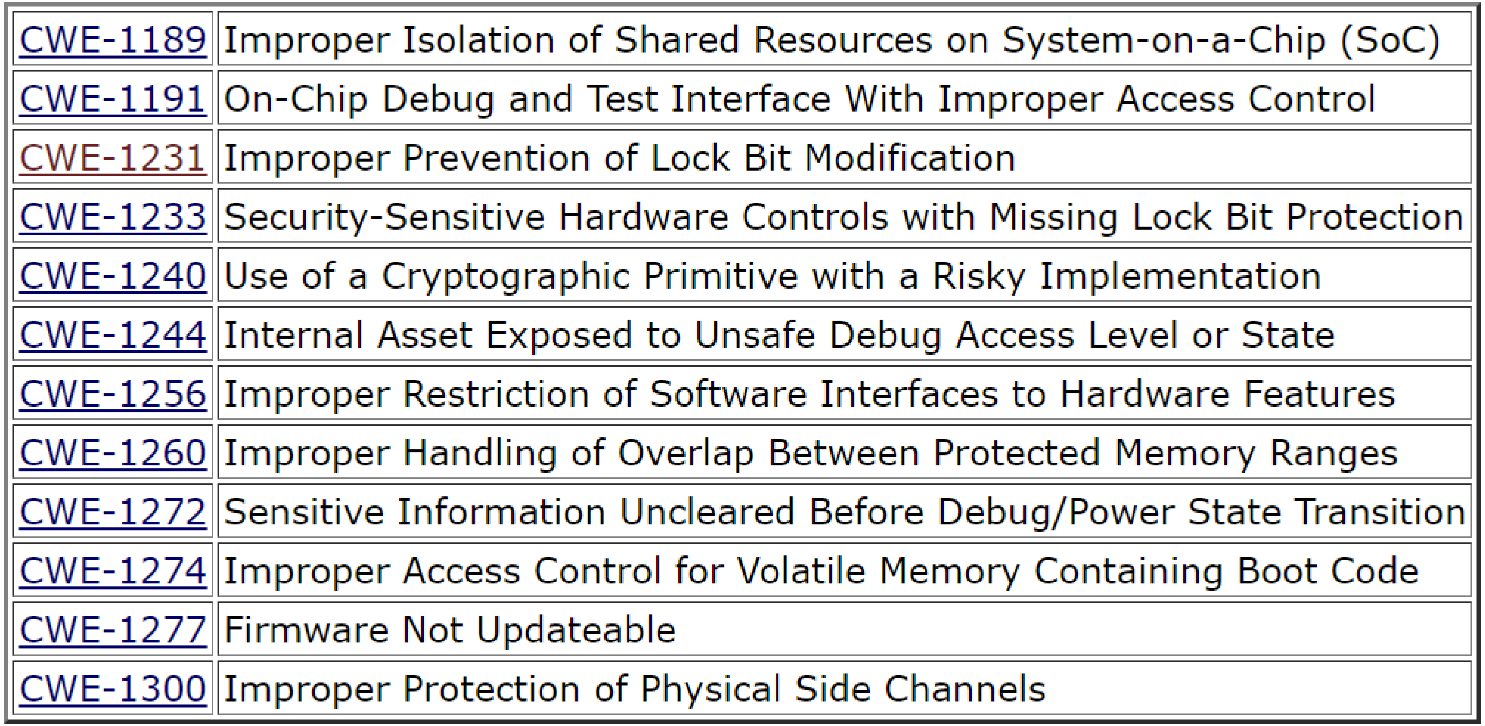
Most Important Hardware Weaknesses Refresh

Bob H

Most Important Hardware Weaknesses (MIHW)

- **Is this something worth revisiting?**
- **Part of CWE 4.6 Release, October 28, 2021**
- **Have there been substantial developments since the last release of MIHW?**
- **Would those affect the rankings and inclusions of the list in any meaningful way?**

Current MIHW



CWE-1189	Improper Isolation of Shared Resources on System-on-a-Chip (SoC)
CWE-1191	On-Chip Debug and Test Interface With Improper Access Control
CWE-1231	Improper Prevention of Lock Bit Modification
CWE-1233	Security-Sensitive Hardware Controls with Missing Lock Bit Protection
CWE-1240	Use of a Cryptographic Primitive with a Risky Implementation
CWE-1244	Internal Asset Exposed to Unsafe Debug Access Level or State
CWE-1256	Improper Restriction of Software Interfaces to Hardware Features
CWE-1260	Improper Handling of Overlap Between Protected Memory Ranges
CWE-1272	Sensitive Information Uncleared Before Debug/Power State Transition
CWE-1274	Improper Access Control for Volatile Memory Containing Boot Code
CWE-1277	Firmware Not Updateable
CWE-1300	Improper Protection of Physical Side Channels

New HW CWEs Since MIHW

- **CWE-1342: Information Exposure through Microarchitectural State after Transient Execution**
- **CWE-1357: Reliance on Insufficiently Trustworthy Component**
- **CWE-1384: Improper Handling of Physical or Environmental Conditions**
- **CWE-1388: Physical Access Issues and Concerns**

Discussion

- **Have there been substantial developments since the last release of MIHW?**
- **Would those affect the rankings and inclusions of the list in any meaningful way?**
- **Are there observational trends that would change the current list in any significant and meaningful way?**

Next Meeting (Sep 8th)

CWE@MITRE.ORG

- **Mailing List:** *hw-cwe-special-interest-group-sig-list@mitre.org*
  - ***NOTE: All mailing list items are archived publicly at:***
    - *https://www.mail-archive.com/hw-cwe-special-interest-group-sig-list@mitre.org/*
- **What would members of this body like to see for the next HW SIG agenda?**
- **Questions, Requests to present? Please let us know.**

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

Backup