# Hardware CWE™ Special Interest Group (SIG)

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

MITRE

September 8, 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** | Call For Help:<br>*HW CWE’s Missing DEMOXs, OBEXs and Mitigations* | Bob H | 5 min |
| **3** | Resonant and Harmonic Based Weaknesses | Gage H | 20 min |
| **4** | Weaknesses dealing with HW initialization<br>*(Nordic APPROTECT)* | Bob H | 20 min |

# Housekeeping

- **Schedule:**
  - **Next Meeting:**
    - **October 13th**
    - **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 October SIG**
- **HW CWE Spotlight: SIG Member to present internal tool developed that utilizes HW CWE.**

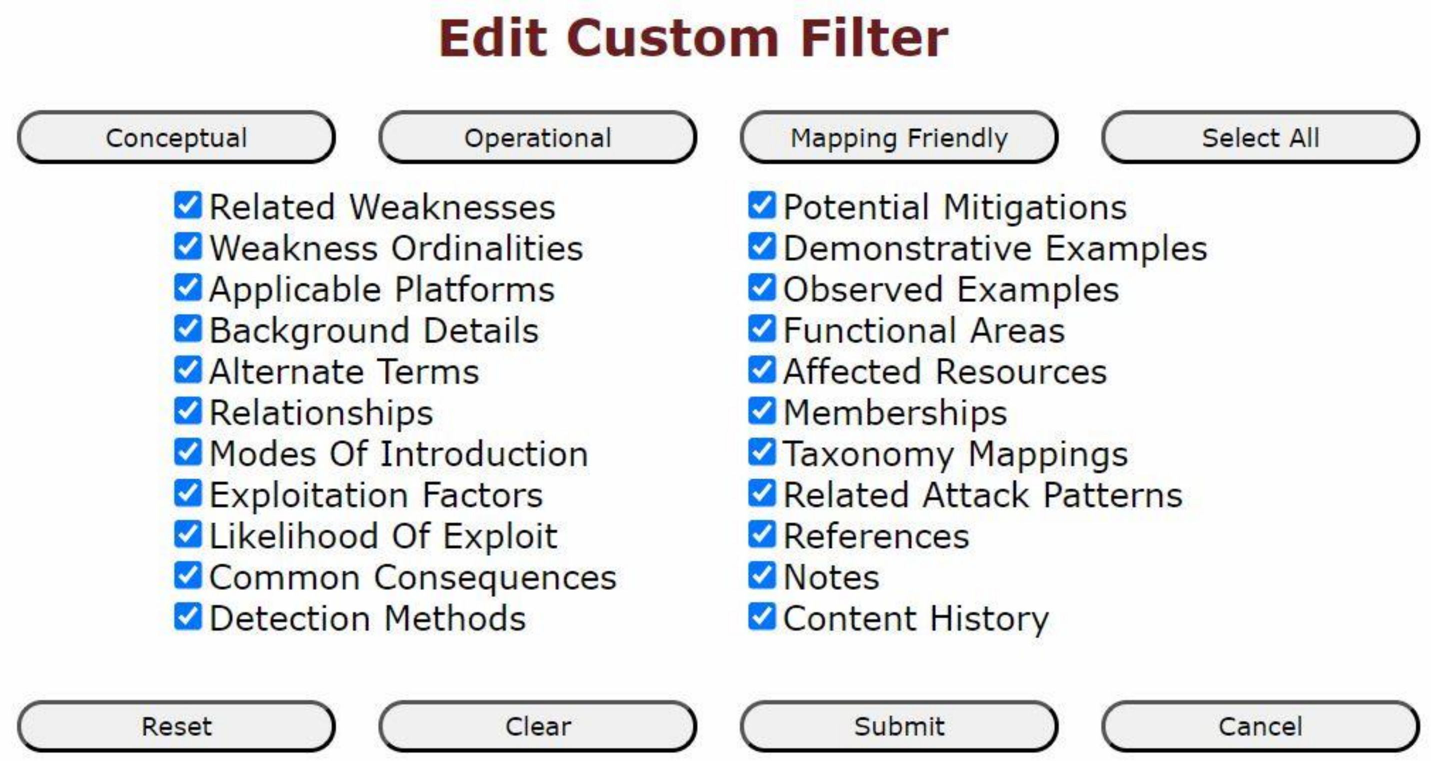
# CWE Nit Bits

*Bite-sized knowledge*
*that will enhance your CWE proficiency!*

# Custom Filtering

- 4.11 added a new “Custom” filter
- Allows users to choose any subset of fields for an entry
- Show weakness details that are most relevant to you
- Filters persist as you navigate through CWE content
- Works with all CWE weakness entries

# Filter Demo



## Edit Custom Filter

- ☑ Related Weaknesses
- ☑ Weakness Ordinalities
- ☑ Applicable Platforms
- ☑ Background Details
- ☑ Alternate Terms
- ☑ Relationships
- ☑ Modes Of Introduction
- ☑ Exploitation Factors
- ☑ Likelihood Of Exploit
- ☑ Common Consequences
- ☑ Detection Methods
- ☑ Potential Mitigations
- ☑ Demonstrative Examples
- ☑ Observed Examples
- ☑ Functional Areas
- ☑ Affected Resources
- ☑ Memberships
- ☑ Taxonomy Mappings
- ☑ Related Attack Patterns
- ☑ References
- ☑ Notes
- ☑ Content History

# Call for Help

## *HW CWE’s Missing DEMOXs, OBEXs and Mitigations*

# HW CWE's With Missing:
## DEMOX's, OBEX's and Mitigations

- **96% of HW CWE entries have mitigations**
  - 4 CWEs are missing mitigations
- **84% of HW CWE entries have demonstrative examples**
  - 17 CWEs do not have any demonstrative examples
  - Intel and Technische Universität Darmstadt are working this.  Will be providing 10 this for this upcoming release.
- **36% of HW CWE entries have observed examples**
  - 67 CWEs do not have any observed examples

- **We will be posting the CWE's with missing elements on the public GitHub. If you have suggestions to fill out these missing elements, we welcome your contributions.**

# CWE Labs

## *Resonant and Harmonic Based Weaknesses*

# Discussion Item

- **Use cases and studies around resonant frequencies and their effects on analog components**
- **Questions and opinions regarding resonant frequencies in CWE:**
  - Are resonant frequencies a topic that should be covered by CWE?
  - What would we consider the weakness to be?
  - Is this research pointing to security, safety, or resiliency concerns?
  - Is there a particular parent CWE that fits?
    - CWE-1384: Improper Handling of Physical or Environmental Conditions?

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

# Resonant Frequency Research Item

- **It was discovered that playing Janet Jackson's *Rhythm Nation* music video on certain laptop model speakers could cause them to crash or cause laptops in the vicinity to crash [1][2] - CVE-2022-38392**
- ***Rhythm Nation* contained a resonant frequency for a 5400 rpm model laptop that was disrupting the laptop's HDD functionality long enough to cause the OS to crash [1][2]**
- **A resonant frequency is defined as "the natural frequency of an object where it tends to vibrate at a higher amplitude" [3]**
- **A 2014 study found that resonant frequencies could cause the HDD platter to vibrate significantly [4] and a 2018 study noted increase in seek errors due to platter dislocation after applying resonant frequencies [5]**

1. *https://devblogs.microsoft.com/oldnewthing/20220816-00/?p=106994*
2. *https://devblogs.microsoft.com/oldnewthing/20220920-00/?p=107201*
3. *https://resources.pcb.cadence.com/blog/2021-what-is-resonant-frequency*
4. *https://docslib.org/doc/9967064/vibration-of-main-components-of-hard-disk-drive-and-the-vibrational-energy-transmission-in-hard-disk-drive*
5. *https://www.princeton.edu/~pmittal/publications/acoustic-ashes18.pdf*

# Resonant Frequency Research

- **In 2022, a study showed how data could be transmitted to an infected smartphone from an air-gapped computer by using sound waves in the resonant frequencies of the smartphone's MEMS gyroscope [1]**

- **In 2009, a study was able to disrupt and lock the ring oscillator used for entropy in a TRNG by injecting resonant frequencies [2]**

- **In 2017, a study showed how playing resonant frequencies near a MEMS accelerometer could disrupt valid results or fabricate false results [3]**

1. *https://arxiv.org/pdf/2208.09764.pdf*
2. *https://www.cl.cam.ac.uk/~atm26/papers/markettos-ches2009-inject-trng.pdf*
3. *https://ieeexplore.ieee.org/document/7961948*

# Discussion

- **Are resonant frequencies a topic that should be covered by CWE?**
- **What would we consider the weakness to be?**
- **Is this research pointing to security, safety, or resiliency concerns?**
- **Is there a particular parent CWE that fits?**
  - CWE-1384: Improper Handling of Physical or Environmental Conditions?
- **NOTE:** A ***Weakness*** is a condition in a software, firmware, hardware, or service component that, under certain circumstances, could contribute to the introduction of vulnerabilities.

# Weaknesses dealing with HW initialization (Nordic APPROTECT)

# Nordic RF Debug and Incorrect Initializations

- **Would like to discuss if we have adequate coverage for incorrect initializations in the HW View.**

- **A motivating example is taken from CVE-2020-27211**
  - “Nordic Semiconductor nRF52840 devices through 2020-10-19 have improper protection against physical side channels. The flash read-out protection (APPROTECT) can be bypassed by injecting a fault during the boot phase.”

- **This refers to physical side channels and is mapped to CWE-203, but that isn’t the best mapping.**

# Nordic RF Debug Disable Details

- **Security feature is called Access Port Protection (APPROTECT).**
- **When APPROTECT is enabled, the debugger is blocked from read and write access to all CPU registers and memory mapped addresses.**
  - SWD is disabled.
- **APPROTECT is enabled by setting some fields in a Non-volatile memory location.**
- **Once set, only a full erase of RAM and flash will disable APPROTECT.**
- **In Rev F of the silicon, APPROTECT is disabled by default.**

# Nordic RF Debug Disable Bypass Details

- **Sometime during the boot process the non-volatile memory is read to configure APPROTECT**
- **There is a time window during the boot process where a power fault can be injected that will cause the APPROTECT enable setting to be ignored, thus allow SWD to continue to be enabled.**
- **The next revision (G) of the chip "by default the, access port protection is enabled".**

*https://limitedresults.com/2020/06/nrf52-debug-resurrection-approtect-bypass/*

# Mapping to a CWE

- **CVE-2020-27211 maps to CWE-203 Observable Discrepancy.**
- **The CVE description uses the phrase "improper protection against physical side channels" which would lead one to map to CWE-1300: Improper Protection of Physical Side Channels.**
- **In this case the side channel of power monitoring is an attacker perquisite to perform the attack.**
- **The root of the issue here is that APPROTECT is disabled by default.**
- **After looking through many different CWEs there are a couple that seem relevant.**

# Potential CWEs

- **CWE-1188: Insecure Default Initialization of Resource**
  - This is a software focused CWE.
- **CWE-1221: Incorrect Register Defaults or Module Parameters**
  - This may fit and it is in the HW View.
  - However, we do not have enough details about the design or how the mitigation was applied to know if this was a change to a register or module parameter.
- **We most likely would have to map to CWE-665: Improper Initialization, which is very abstract and discouraged for mapping.**

# Discussion

**This has highlighted a gap.**

- **(P) CWE-664: Improper Control of a Resource Through its Lifetime**
  - (C) CWE-665: Improper Initialization
    - *(C) CWE-TBD: Incorrect Initialization of Resource*
      - (B) CWE-1188: Insecure Default Initialization of Resource
      - (B) CWE-1221: Incorrect Register Defaults or Module Parameters

- **Would this be useful for you?**
- **Are there other scenarios in HW design where there are initialization mistakes that aren't registers or module parameters?**
- **Is this something we should add to the HW View?**

# Next Meeting (Oct 13th)

**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.**

# Backup