Hardware CWE™ Special Interest Group (SIG)

Chair: Bob Heinemann (MITRE)

Co-Chair: “Manna” Parbati Kumar Manna (Intel)

MITRE Team: Gananand Kini, Steve Christey Coley, Alec Summers

MITRE

March 14, 2025

Agenda

REMINDER: This meeting is being recorded.

1	General Status of Current HW CWE Submissions	Steve Christey	15 min
2	HW Crypto Leak Submission Review	Andres Meza	20 min
3	Most Important Hardware Weaknesses Refresh Update	Arun K, Ganu K	10 min

Housekeeping

- **Schedule:**
  - **Next Meeting April 11:**
    - **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

- **CWE 4.16 has been released. Includes the 2024 Top 25.**
- **CWE 4.17 planned for release April 3, 2025. Content freeze on March 31, 2025.**
- **CWE Content Development Repository (CDR) to be made public with CWE 4.17 release.**

Call for Topics

What topics should we cover next time?

- **Anything to share today or topics for consideration for next meeting?**

Hardware Submissions in Progress

- **Initial Consultation (Stage 1, Phase 4 – common bottleneck)**
  - HW/SW: ES2306-c0b52346 Use of a Quantum-Vulnerable Cryptographic Algorithm (NIST)
- **Ready for Acceptance (Stage 1, Phase 6)**
  - ES2208-9fb81a1a Speculative propagation of requests for transaction before data validation in multi-manager bus architectures (Francesco Restuccia)
- **Details Received (Stage 2, Phase 8)**
  - ES2208-26ac7ee6 Improper Protection of Intermediate Cryptographic State/Results (Andres Meza)
- **Detailed Consultation (Stage 2, Phase 10)**
  - ES2312-c2337436 Lack of Feedback for Unexecuted Operations Across System Interfaces (Amisha Srivastava)
- **See CDR: https://github.com/CWE-CAPEC/CWE-Content-Development-Repository/issues**

Update: Lack of Feedback for Unexecuted Operations Across System Interfaces

- **CWE Team worked with Amisha Srivastava to address HW-SIG comments**
- **Changes not finalized**
- **Name changes**
  - Previous: “Lack of Feedback for Unexecuted Operations Across System Interfaces”
  - Current: “Missing Security-Critical Feedback for Unexecuted Operations”
- **Short description (1 or 2 sentences)**
  - The product has a hardware interface that silently discards operations in situations for which feedback would be security-critical. While intentional omission of feedback can be a valid security strategy when it is clearly defined and controlled, feedback not being reported is a critical weakness when its absence prevents the timely detection of failures or attacks.
- **Still developing examples with clear security implications**

HW CWE Submission

Andres Meza

Most Important Hardware Weaknesses (MIHW) Refresh Update

Gananand Kini

Most Important Hardware Weaknesses Refresh – March 2025 Update

- **In the process of collecting data on CVEs related to HW CWEs**
- **Deadline to finish data collection by end of next week (~March 21, 2025)**
- **Two sources of data: existing vulnerabilities, and expert opinion**
- **Combine both, but how?**
  - Data & Expert Opinion
    - If both data and expert opinion point to a particular CWE, it should be included on the MIHW list.
  - No Data & Expert Opinion
    - If experts identify a CWE not highlighted by the data, but expert consensus is strong, include it with a note on expert-driven inclusion.
  - Data & No Expert Opinion
    - If data indicates a weakness but experts do not prioritize it, then it should not be included in the MIHW list.
  - No Data & No Expert Opinion
    - Exclude CWE from the MIHW list, as there is no supporting evidence or expert consensus.

Most Important Hardware Weaknesses Refresh – March 2025 Update contd…

- **Next steps**
  - Figure out how to collect expert opinion from the HW CWE SIG
  - Compile the list by applying methodology
  - Coordinate communications of the final compiled list

MIHW List Discussion

- **Please continue discussion on the HW CWE Mailing List (see below).**
  - You can tag email subject lines using "[MIHW]" to get more visibility.

- **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/*

Next Meeting (April 11)

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

Popular CWEs in NVD excluding Software CWEs

- **33 unique HW CWEs with *at least* 1 CVE in NVD.**
- **16 HW CWEs with *only* 1 CVE**
- **11 HW CWEs with 2 CVEs**

13	CWE-1220: Insufficient Granularity of Access Control
4	CWE-1320: Improper Protection for Outbound Error Messages and Alert Signals
3	CWE-1357: Reliance on Insufficiently Trustworthy Component
3	CWE-1295: Debug Messages Revealing Unnecessary Information
3	CWE-1258: Exposure of Sensitive System Information Due to Uncleared Debug Information
3	CWE-1240: Use of a Cryptographic Primitive with a Risky Implementation
2	CWE-1332: Improper Handling of Faults that Lead to Instruction Skips
2	CWE-1319: Improper Protection against Electromagnetic Fault Injection (EM-FI)
2	CWE-1303: Non-Transparent Sharing of Microarchitectural Resources
2	CWE-1299: Missing Protection Mechanism for Alternate Hardware Interface
2	CWE-1298: Hardware Logic Contains Race Conditions
2	CWE-1281: Sequence of Processor Instructions Leads to Unexpected Behavior
2	CWE-1279: Cryptographic Operations are run Before Supporting Units are Ready
2	CWE-1269: Product Released in Non-Release Configuration
2	CWE-1263: Improper Physical Access Control

Formation of Ad-Hoc Committee

- **Will be putting a call out of the mailing list for members to join an ad-hoc committee to study.**
- **We will be looking for committee members to study the feasibility of a new list and making a decision to proceed.**
- **Also, members will develop an approach to develop the list with the community.**

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?
- Is there any data available that we could utilize to generate the list? Or should we use the delphi method again?
- Are there observational trends that would change the current list in any significant and meaningful way?

Current MIHW from CWE 4.6 (Unranked)

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

Previous Methodology for the MIHW

- **Previously, the Delphi method was used to poll members of this august body:**
  - Which 10 HW weaknesses were important based on nine significance questions:
    1. How frequently is this weakness detected after it has been fielded?
    2. Does the weakness require hardware modifications to mitigate it?
    3. How frequently is this weakness detected during design?
    4. How frequently is this weakness detected during test?
    5. Can the weakness be mitigated once the device has been fielded?
    6. Is physical access required to exploit this weakness?
    7. Can an attack exploiting this weakness be conducted entirely via software?
    8. Is a single exploit against this weakness applicable to a wide range (or family) of devices?
    9. What methodologies do you practice for identifying and preventing both known weaknesses and new weaknesses?

Previous Methodology for MIHW

- **After combining the above, thirty-one unique weaknesses resulted.**
- **Live poll conducted during SIG meeting asked members to assign the thirty-one into various buckets with weights (strongly support (+2), somewhat support (+1), no opinion (0), somewhat oppose (-1), strongly oppose (-2)).**
- **Multiple groups emerged from the data when ranked by weighted percentage of votes, of which the primary group contained twelve. The secondary group were listed as Hardware Weaknesses on the Cusp (shown below).**

CWE-226	Sensitive Information in Resource Not Removed Before Reuse
CWE-1247	Improper Protection Against Voltage and Clock Glitches
CWE-1262	Improper Access Control for Register Interface
CWE-1331	Improper Isolation of Shared Resources in Network On Chip (NoC)
CWE-1332	Improper Handling of Faults that Lead to Instruction Skips

Changes to HW CWEs since MIHW (v4.6 to v4.16)

- (DEPRECATED) CWE-1324: Sensitive Information Accessible by Physical Probing of JTAG Interface
- CWE-1342: Information Exposure through Microarchitectural State after Transient Execution
- (Class) CWE-1357: Reliance on Insufficiently Trustworthy Component
  - CWE-1329: Reliance on Component That is Not Updateable
- (Class) CWE-1384: Improper Handling of Physical or Environmental Conditions
- (Category) CWE-1388: Physical Access Issues and Concerns
- (Parent) CWE-1420: Exposure of Sensitive Information during Transient Execution
  - CWE-1421: Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution
  - CWE-1422: Exposure of Sensitive Information caused by Incorrect Data Forwarding during Transient Execution
  - CWE-1423: Exposure of Sensitive Information caused by Shared Microarchitectural Predictor State that Influences Transient Execution
- This list is not complete!

Questions to think about and frame the MIHW activity

- **Unfortunately, not many HW CWEs assigned to CVE entries in NVD currently.**
- **A lot of the observed examples (CVE) were added mostly for Transient Execution weaknesses. There are many that remain incomplete.**
- **What methodology should be used for the new MIHW list?**
- **What data could be used to generate the new MIHW list?**
- **Any observations or lessons learned that could change or impact the current list in a meaningful way? Any observed trends that could impact the list?**
- **Does it capture the use cases and important attributes discussed earlier for such a list?**