Hardware CWE™ Special Interest Group (SIG)

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

MITRE

July 14, 2023

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

Agenda

REMINDER: This meeting is being recorded.

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

1	CWE Nit Bits	Bob H	5 min
2	CWE 4.12 Release Summary and new Demox's	Bob H	10 min
3	Becoming a CNA	Alec S	20 min
4	Status of HW CWE Submissions	Steve C	15 min
5	Most Important Hardware Weaknesses Refresh	Bob H	10 min

Housekeeping

- **Schedule:**
  - **Next Meeting:**
    - **Reschedule from Aug 11 to Aug 18**
    - **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

- **Top 25 Release June 29**
- **CWE 4.12 Release June 29**
- **Tentative: CISA strategy around Secure By Design/Secure By Default for Aug SIG**

CWE Nit Bits

Bite-sized knowledge
that will enhance your CWE proficiency!

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

Common Terms Cheatsheet

- **Did you ever wonder what the difference between a Pillar, Class, Base and Variant weakness is?**
- **How about common terms found in weakness titles, such as:**
  - Resource, Information Exposure, Improper, Authentication and Authorization
- **There is a Common Terms Cheatsheet**
  - https://cwe.mitre.org/documents/cwe_usage/common_terms_cheatsheet.html

CWE 4.12 Release Summary and new Demox’s

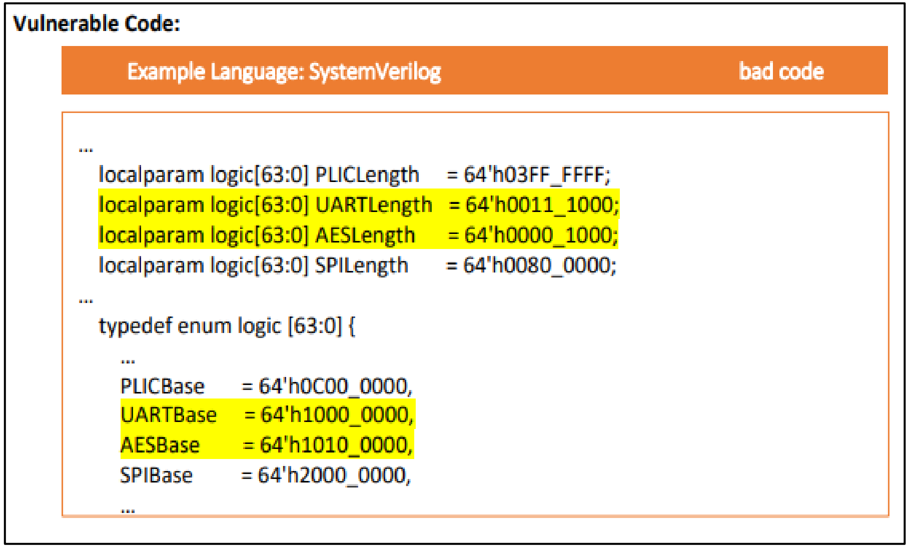
Bob H

New in 4.12

- **Top 25 was major focus of 4.12**
- **During mapping process there were a few mappings to specific HW CWEs.**
  - About 10 out of over 7000+
  - Looking through to see if any can be used as OBEXs.
- **New HW DEMOX's**
  - Hardware-specific demonstrative examples derived from Hack@DAC 2019, with input from Technical University of Darmstadt, Texas A&M University, Intel (Jason Fung) and the Hardware CWE Special Interest Group (HW CWE SIG).
- **New DEMOX's include Github links to see snippet code in full context**

CWE-1260: Improper Handling of Overlap Between Protected Memory Ranges

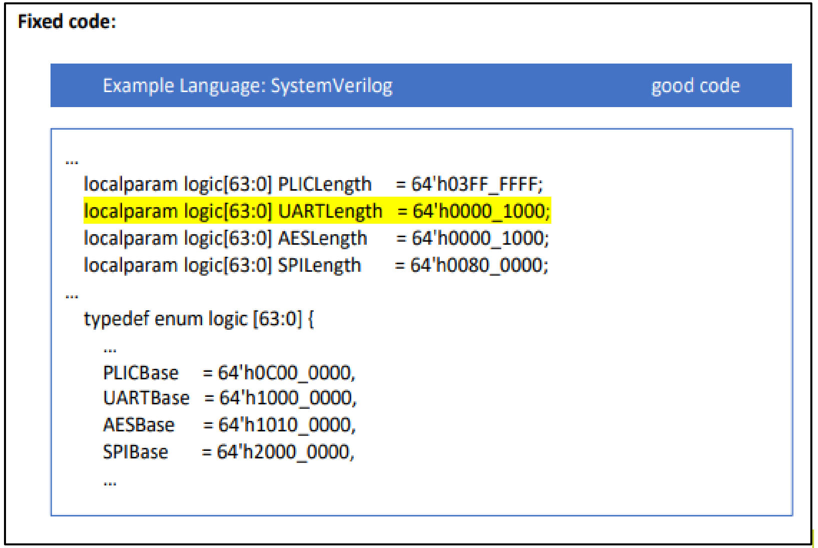
…Access to the AES IP MMIO region is considered privileged as it provides access to AES secret key, internal states, or decrypted data. The vulnerable code allows the overlap between the protected MMIO region of the AES peripheral and the unprotected UART MMIO region…



Vulnerable Code:

Example Language: SystemVerilog	bad code

```
...
  localparam logic[63:0] PLICLength    = 64'h03FF_FFFF;
  localparam logic[63:0] UARTLength    = 64'h0011_1000;
  localparam logic[63:0] AESLength     = 64'h0000_1000;
  localparam logic[63:0] SPILength     = 64'h0080_0000;
...
  typedef enum logic [63:0] {
    ...
    PLICBase     = 64'h0C00_0000,
    UARTBase     = 64'h1000_0000,
    AESBase      = 64'h1010_0000,
    SPIBase      = 64'h2000_0000,
    ...
```



Fixed code:

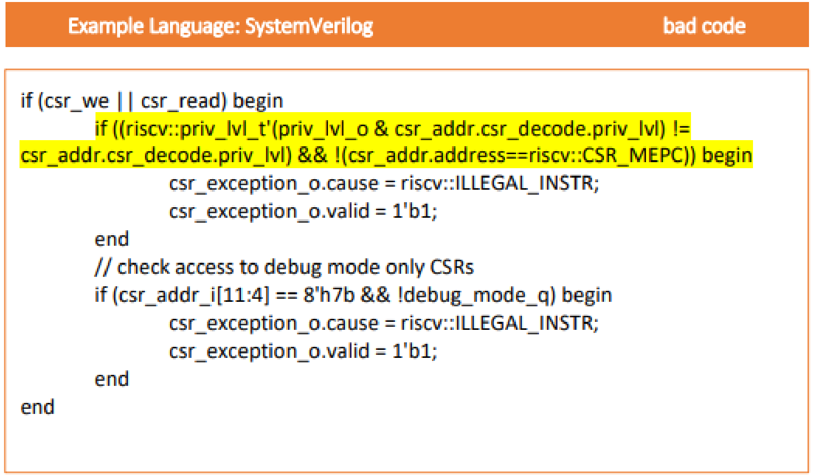
Example Language: SystemVerilog	good code

```
...
  localparam logic[63:0] PLICLength    = 64'h03FF_FFFF;
  localparam logic[63:0] UARTLength    = 64'h0000_1000;
  localparam logic[63:0] AESLength     = 64'h0000_1000;
  localparam logic[63:0] SPILength     = 64'h0080_0000;
...
  typedef enum logic [63:0] {
    ...
    PLICBase    = 64'h0C00_0000,
    UARTBase    = 64'h1000_0000,
    AESBase     = 64'h1010_0000,
    SPIBase     = 64'h2000_0000,
    ...
```

CWE-1262: Improper Access Control for Register Interface

…The vulnerable example code **allows the machine exception program counter (MEPC) register to be accessed from a user mode program by excluding the MEPC from the access control check.** MEPC as per the RISC-V specification can be only written or read by machine mode code. Thus, the attacker in the user mode can run code in machine mode privilege (privilege escalation)….

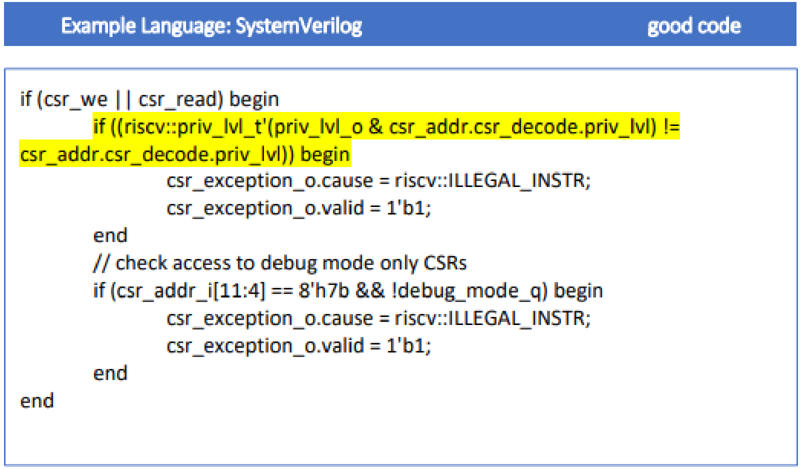
Vulnerable Code:



Example Language: SystemVerilog bad code

```
if (csr_we || csr_read) begin
        if ((riscv::priv_lvl_t'(priv_lvl_o & csr_addr.csr_decode.priv_lvl) !=
csr_addr.csr_decode.priv_lvl) && !(csr_addr.address==riscv::CSR_MEPC)) begin
                csr_exception_o.cause = riscv::ILLEGAL_INSTR;
                csr_exception_o.valid = 1'b1;
        end
        // check access to debug mode only CSRs
        if (csr_addr_i[11:4] == 8'h7b && !debug_mode_q) begin
                csr_exception_o.cause = riscv::ILLEGAL_INSTR;
                csr_exception_o.valid = 1'b1;
        end
end
```

Fixed code:

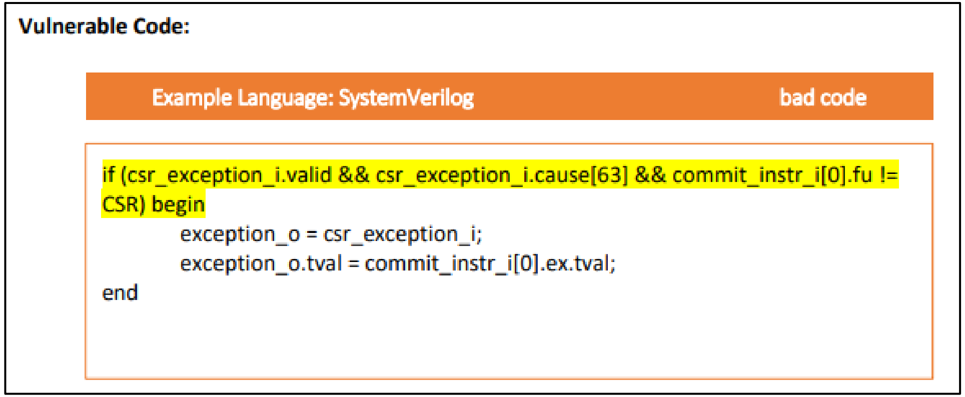


Example Language: SystemVerilog good code

```
if (csr_we || csr_read) begin
        if ((riscv::priv_lvl_t'(priv_lvl_o & csr_addr.csr_decode.priv_lvl) !=
csr_addr.csr_decode.priv_lvl)) begin
                csr_exception_o.cause = riscv::ILLEGAL_INSTR;
                csr_exception_o.valid = 1'b1;
        end
        // check access to debug mode only CSRs
        if (csr_addr_i[11:4] == 8'h7b && !debug_mode_q) begin
                csr_exception_o.cause = riscv::ILLEGAL_INSTR;
                csr_exception_o.valid = 1'b1;
        end
end
```

CWE-1281:
Sequence of Processor Instructions Leads to Unexpected Behavior

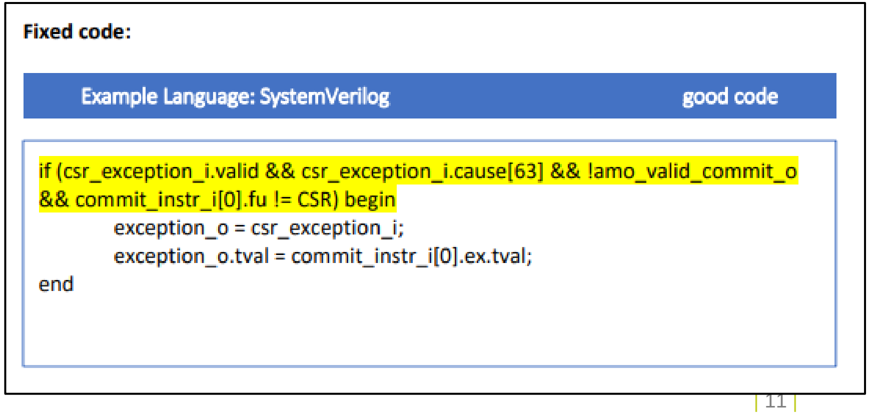
…The following vulnerable code check for CSR interrupts and give them precedence over any other exception. However, **the interrupts should not occur when the processor runs a series of atomic instructions.** In the following vulnerable code, the required check must be included to ensure the processor is not in the middle of a series of atomic instructions. For more info, please check the Fixed code example…



Vulnerable Code:

Example Language: SystemVerilog bad code

```
if (csr_exception_i.valid && csr_exception_i.cause[63] && commit_instr_i[0].fu !=
CSR) begin
          exception_o = csr_exception_i;
          exception_o.tval = commit_instr_i[0].ex.tval;
end
```



Fixed code:

Example Language: SystemVerilog good code

```
if (csr_exception_i.valid && csr_exception_i.cause[63] && !amo_valid_commit_o
&& commit_instr_i[0].fu != CSR) begin
          exception_o = csr_exception_i;
          exception_o.tval = commit_instr_i[0].ex.tval;
end
```

38 Potential New HW DEMOX’s

- 4.12 HW DEMOX’s came in as a batch of 3
- Format is good for us to easily incorporate into CWE
- Hack@DAC’19 and Hack@DAC’21 covered 38 unique HW CWE’s
- Looking forward to receiving additional batches to incorporate
- As new batches come in it would be great for HW SIG members to review for correctness and suggestions to clarify text if needed.

Becoming a CNA
Alec S

CVE Numbering Authority (CNA) Information and Requirements

GET AHEAD OF BOOM!

CWE
CVE
Common Vulnerabilities and Exposures

Weaknesses

The root cause of a vulnerability

CWE-79: Improper Neutralization of Input During Web Page Generation

Vulnerabilities

Specific instances of a weakness type that are demonstrably exploitable

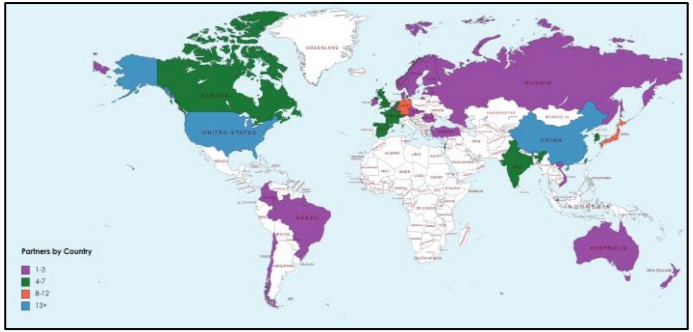
2000+ Cross Site Scripting Vulns in specific technologies in 2022

What is a CVE Numbering Authority (CNA)?

- **CVE Numbering Authority (CNA):** Organizations from around the world who are authorized by the CVE Program to assign CVE IDs and publish CVE Records for vulnerabilities within their distinct, agreed-upon scope.
  - Types of organizations include vendors, researchers, open source, CERTs, hosted services, bug bounty providers, and consortiums, but others are also welcome.

Strategy of Federation in Action

As of July 14, 2023:
304 Partners in 36 countries



Federated Growth Strategy Implemented

Federation Through Partnership: Impact by the Numbers		
Year	**Records Published**	**Number of CNAs**
2016	**6,457**	**24 (1 Int.)**
2017	**14,644**	**78**
2018	**16,510**	**90**
2019	**17,308**	**106**
2020	**18,364**	**144**
2021	**20,161**	**209 (100 Int.)**
2022	**25,059**	**263 (123 Int.)**
2023	**11,805**	**295 (136 Int.)**

Year	1999-2016	2017	2018	2019	2020	2021	2022	2023
All CNAs	0%	50%	53%	53%	58%	65%	68%	77%
CNA-LRs	100%	50%	47%	47%	42%	35%	32%	23%

***Note: CISA ICS became a Top-Level Root and CNA-LR in calendar year 2020**

***Note: 57 CNAs Added, to-date in FY 2023**

Benefits of Becoming a CNA

- **Demonstrate mature vulnerability management practices and commitment to cybersecurity**
- **Communicate value-added vulnerability information**
  - You are the subject matter experts and can provide the most accurate vulnerability description
- **Control the CVE publication release process for vulnerabilities within scope**
- **Assign CVE IDs without having to share embargoed information with another CNA**
- **Streamline vulnerability disclosure processes**

Cost of Being a CNA

- **There is no monetary fee; however, CVE Records are not free to produce (i.e., time and resource allocation)**
  - Estimated minimum Level of Effort: 8 hours per month (up to 10 CVE Records)
- **CNAs volunteer their own time for their own benefit**
- **No contract to sign**

Requirements for becoming a CNA

- Have a public vulnerability disclosure policy* (e.g., Microsoft)
- Have a public advisory location (e.g., Apple)
- Agree to the CVE Program Terms of Use

Please visit https://www.cve.org/PartnerInformation/ListofPartners for examples of other disclosure policies and advisory locations.

Process for Becoming a CNA (1 of 2)

- **Request information on how to become a CNA via the CVE Program webform here**
  - Select "Request information on the CVE Numbering Authority (CNA) Program" from the dropdown menu
- **Your request will be assigned to someone on the Program Coordination team, who will provide a link to the registration form and supplemental material**
  - CNA Rules
  - Onboarding videos
- **Once registration form is received, a one-hour onboarding session will be scheduled**
  - Public vulnerability disclosure policy is required (e.g., Microsoft)
  - Public source for vulnerability disclosures is required (e.g., Apple)
  - Choose Root (or Top-Level Root) based on scope
  - Define scope*

*Please visit https://www.cve.org/PartnerInformation/ListofPartners for examples of scopes.

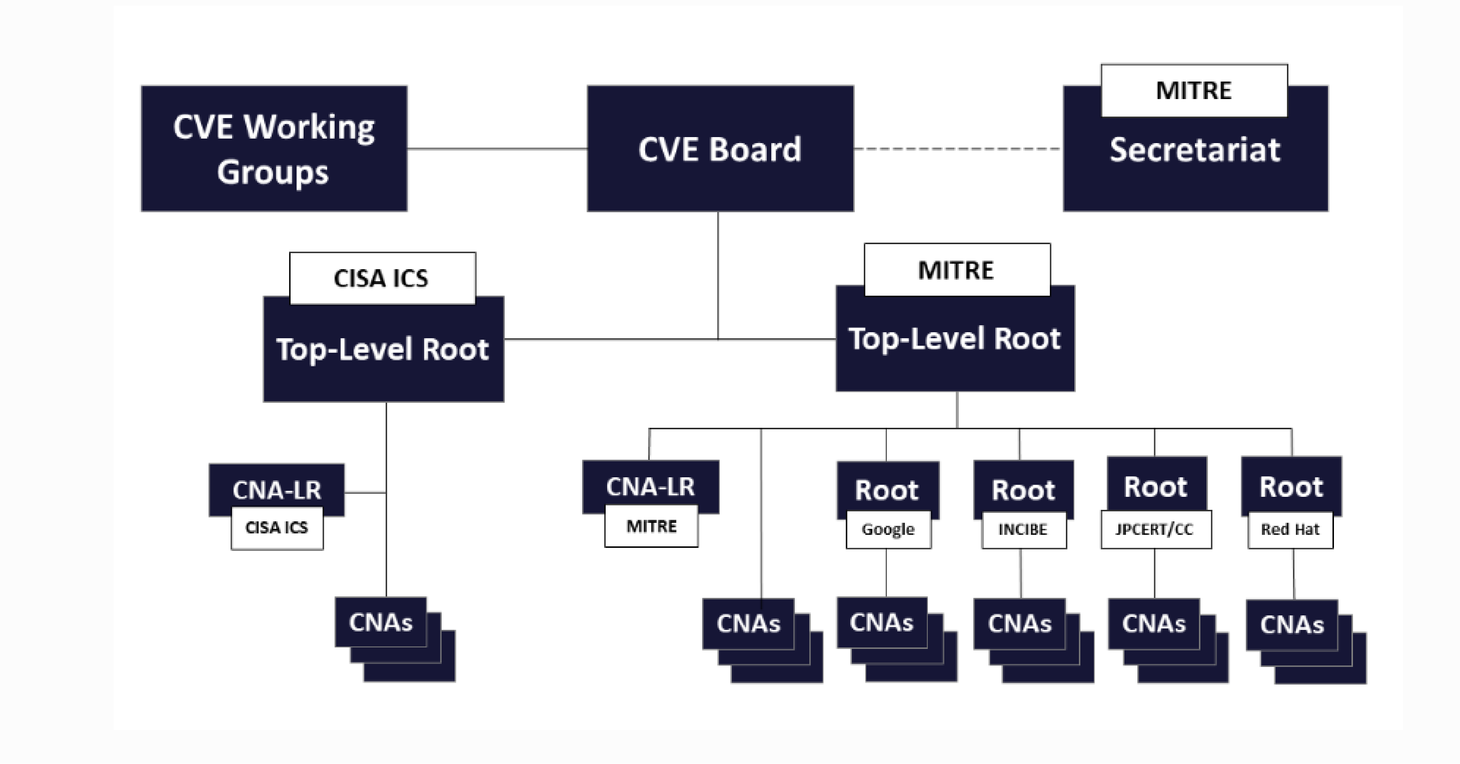
Process for Becoming a CNA (2 of 2)

- **After onboarding session, you will be asked to complete and submit homework**
- **Once homework is submitted and approved, the CVE Program will work with you to select a date for announcement into the program**
- **After official announcement, CNA requests credentials to access CVE Services**
  - Request CVE IDs
  - Publish and update CVE Records

CVE Program Expectations of CNAs

- **Follow the CNA Rules and the CVE Program Professional Code of Conduct**
- **Adhere to the CVE Program policies**
  - Record Dispute Policy
  - EOL Policy
- **Publish CVE Records in a timely manner once disclosure is made public**
  - Once the vulnerability (and associated CVE ID) is made **public** (via an advisory, Tweet, blog, etc.), CVE Records must be published to the CVE List within 5 business days
- **Respond to requests from Root (or Top-Level Root) in a timely manner**
- **Communicate any changes to CNA organization (POCs, mergers, change in scope) to Root or Top-Level Root**

CVE Program Organization



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

Status of HW CWE Submissions
Steve C

Hardware Submission Status Summary

- **We are tracking 13 active hardware submissions for new entries**
- **Most submissions were made before creation of the external submission server and a formalized review process in mid-2022**
  - This review process is detailed but “unwieldy” as-implemented
    - Back-and-forth Q&A style email discussions on complex topics; extensive “checklists” that avoid low-quality submissions but are “expensive”
- **High-level status summary**
  - 2 submissions: “Complex Domain / Classification”
  - 4 submissions: “Overlap / Subtree Overhaul (Access Control)”
  - 1 submission: “Overlap / Subtree Overhaul (Cryptography)”
  - 4 submissions: “Affected by Scope Exclusions”
  - 2 submissions: “Needs integration into existing content”
- **Question for the SIG: which of these are most important to resolve?**

Active Submissions: Complex Domain / Classification

- **HCWE109 / ES2204-e1e55bce: Non-transparent behavior of microarchitectural features**
  - Submitter: Intel
  - Status: informal working group still wrestling with this. Could be 3 or 4 new CWEs; potential overlap with 5+ other CWEs.

- **HCWE111 / ES2208-9fb81a1a - Speculative propagation of requests for transaction before data validation in multi-manager bus architectures**
  - Submitter: Francesco Restuccia, UCSD
  - Status: complicated. Might be overlap with existing microarchitectural work, "side channels," information leaks, etc.

Active Submissions: Overlap / Subtree Overhaul (Access Control)

- **HCWE10 - Incorrect access control policy**
  - Submitter: Intel
  - Status: it's complicated. Part of CWE-284 pillar Improper Access Control. Significant overlap with existing CWEs related to authorization, authentication, etc. Could effectively impose another layer into existing hierarchy and introduce complexity with multiple dimensions of abstraction (missing/incorrect AND behavior and possibly technology). Part of ongoing access-control overhaul.
- **HCWE11 - Missing access control policy**
  - Submitter: Intel
  - Status: it's complicated. See HCWE10 :)
- **HCWE14 - Untrusted Agents Given Access to a Sensitive Asset**
  - Submitter: Intel
  - Status: complicated. Appears to be authorization, although that word is not used. May be focused more on "errors happen in this type of technology" (hardware agents) instead of behavior.
- **HCWE13 - Trusted Agents Excluded from Accessing a Sensitive Asset**
  - Submitter: Intel
  - Status: complicated. Unclear how this is a weakness.

Cryptography-Related

- **CWE has a small team focused on cryptography (whether software or hardware)**
  - Cryptography itself needs improvement and/or restructuring across CWE
- **Overlap / Subtree Overhaul (Cryptography)**
  - **HCWE110 / ES2208-26ac7ee6 Improper Protection of Intermediate Cryptographic State/Results**
    - Submitter: Andres Meza
    - Status: complicated. Likely overlap with other cryptographic weaknesses
- **Needs integration into existing content**
  - **HCWE34 - Secret Leakage in Crypto Primitives**
    - Submitter: Parbati K. Manna
    - Status: deemed not a weakness. Still active because some content could be used in other CWEs (e.g., the demonstrative example may be good for storage in registers)
  - **HCWE33 - Crypto Primitives Not Resistant to Side Channel Attacks**
    - Status: merged into CWE-203, but still active to see if the original submission had additional content to merge into CWE. Requires resolution to larger conversations about side channels. Possible overlap with CWE-1240: Use of a Cryptographic Primitive with a Risky Implementation. Not hardware-specific.

Affected by Scope Exclusions

- **Most/all of these submissions need community-wide discussion and resolution for scope exclusions**
- **HCWE102: Untrusted Manufacturing of Intellectual Property (IP)**
  - Submitter: Paul Wortman
  - Status: Scope issues
- **HCWE103: Lack of Verifiable Testing**
  - Submitter: Paul Wortman
  - Status: Scope issues. Portions related to "golden standard" integrated into CWE-1059: Insufficient Technical Documentation.
- **HCWE104: Missing protective measures for preventing or hindering reverse engineering of IP or other sensitive data**
  - Submitter: Paul Wortman
  - Status: scope issues.
- **HCWE105: Inability to Detect and Prevent Intrusive and Malicious Alterations to Hardware (i.e., Hardware Trojans)**
  - Submitter: Paul Wortman
  - Status: Scope issues; “detecting attack” overlaps many weaknesses; see CWE-507: Trojan Horse

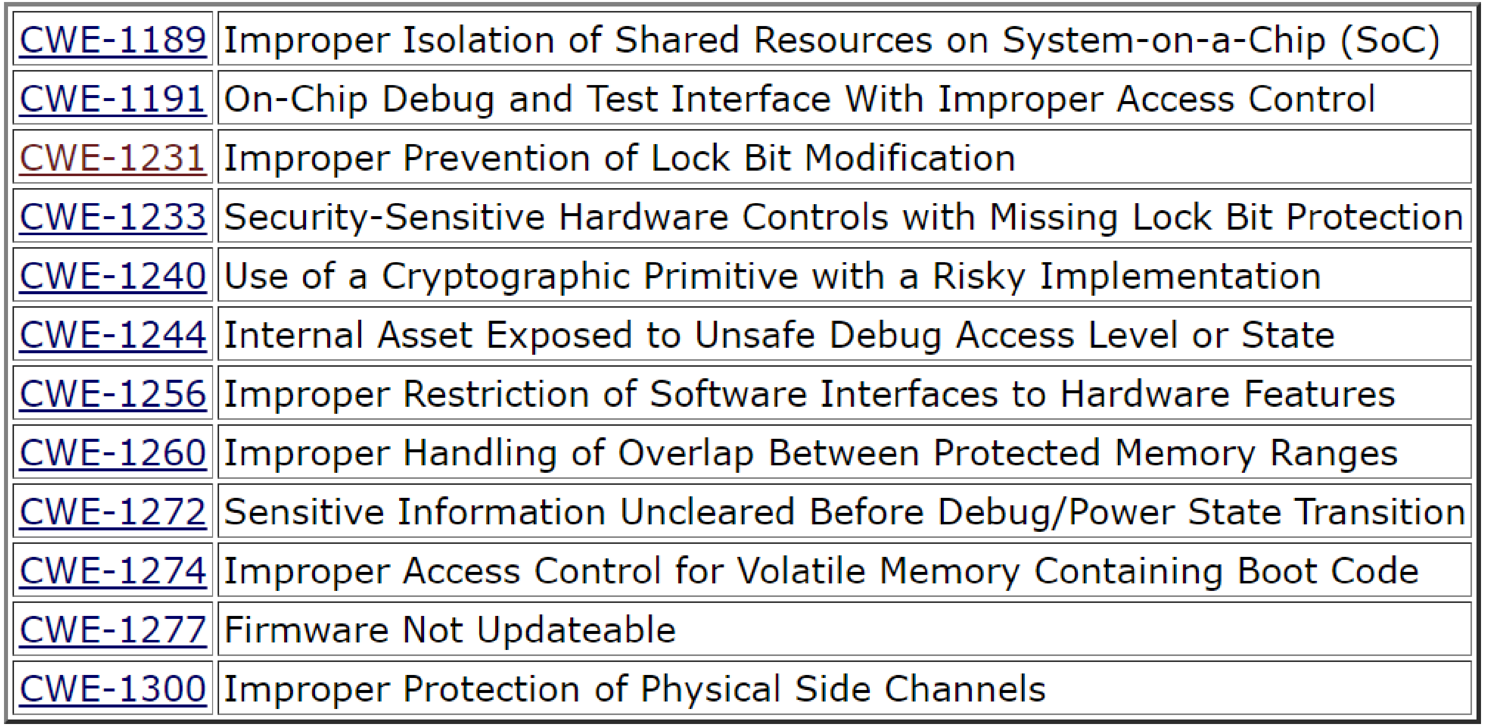
Most Important Hardware Weaknesses Refresh

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**

Next Meeting (Aug 18)

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

CWE-514: Covert Channel

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.

Covert Channels and Side Channels

- This is a discussion item on the GitHub
- Accidental transmission vs intentional transmission
- "A side channel is where information **leaks accidentally** via some medium that was not designed or intended for communication; a covert channel is where the **leak is deliberate.**" – *Ross Anderson*
- Hardware view should have coverage in the hardware view –*Jason Oberg*
- CWE-514 is a class weakness for Covert Channels
- Covert Channels should be in the HW categories Security Flow Issues, General Circuit and Logic Design Concerns, or Debug and Test Problems. –*Paul Wortman*
- Should we place CWE-514 in the HW View? Or create a base of CWE-514 and put that into the HW view?