Hardware CWE™ Special Interest Group (SIG)

Chair: Bob Heinemann (MITRE)

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

MITRE Team: Gage Hackford, Steve Christey Coley, Alec Summers

MITRE

August 9, 2024

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

Agenda

REMINDER: This meeting is being recorded.

1	Call for Topics	Manna	10 min
2	Covert Channels Discussion Close out	Manna	20 min
3	System Verilog vs Verilog Discussion	Gage	20 min
4	Usability Updates and HW CWEs Discussion	Gage	10 min

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

Housekeeping

- Schedule:
  - Next Meeting: Sep 13
    - 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 Content Development Repository (CDR) pilot now on GitHub! Open to anyone by request. Public access in the next few months.**
- **CWE 4.15 release has been released July 16.**
- **CWE 4.16 release is planned for October.**
- **CWE 5.0 is planned for early 2025.**

Call for Topics

What topics should we cover next time?

- **What SIG members shared in July**
  - **Dan Dimase** mentioned weekly Articles of Security interest. Some articles deal with hardware security. ***Looking for volunteer*** to scan those and raise HW related articles to the HW SIGs attention.
  - **Hareesh Khattri** highlighted academic work that uses CWE content LLMs to automate generation of security assertions.

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

Covert Channels Closeout

Covert Channels Discussion Summary

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*
- CWE-514 as currently written it’s specific to software and would need to be tweaked *–Bruce Monroe*
- **May / June HW SIG Meeting**
  - Bob / Manna presented current CWE coverage on covert channels as well as the concept of incidental channels
- **July HW SIG Meeting**
  - Hareesh discussed the importance of considering designers intent when considering covert channels. Suggested that this should be considered for the relationships to the CWE covert channel entry CWE-514.

Covert Channel Closeout – Last Call for Comments

- **What other aspects of Covert Channels and HW CWE should we consider?**

- **Next steps are for the MITRE CWE team and SIG Co-Chair to consider comments and make a proposal for HW SIG consideration.**

System Verilog

System Verilog and Verilog

- Hack@DAC DEMOXs had indicated code snippets were System Verilog.
- The language enumeration in the current schema does not contain System Verilog, just Verilog.

Questions to SIG:

- What is the difference between Verilog and System Verilog?
- Is that difference significant enough that we should add System Verilog to the schema enumeration?
  - For example, we distinguish between C and C++ but not between variants of C (e.g., C89 vs C99).

Usability Updates and HW CWEs Discussion

Usability Task Micro Updates Initial Goals

Above the fold (before the webpage scroll point):

- **Important and concise text is above the fold so the reader can easily scan and digest**

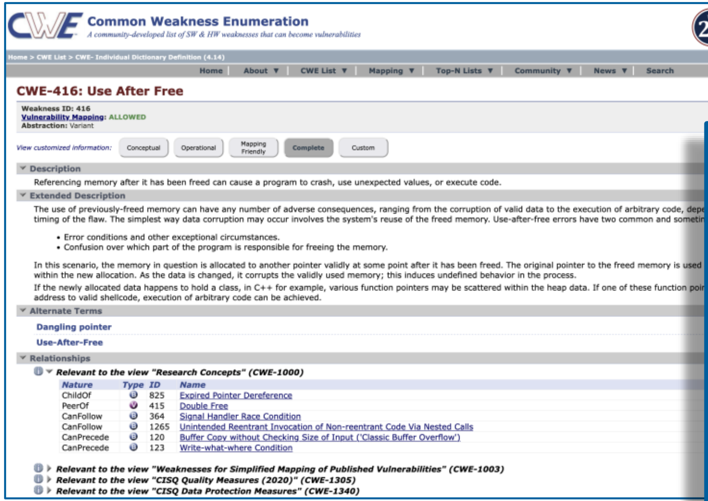
Points to Make Above the Fold:

- **Describe just the weakness and provide a visual aid**
  - Concise summary of weakness (only in description, no extended description)
  - Describe the condition and some context about the condition
  - Concise is 3 – 4 sentences. Images will provide additional context.

Reorder Elements:

- **Alternate Terms**
- **Consequences Element** (bad outcomes)
- **Mitigations Element (**what to do about the weakness)
- Remaining Elements follow

Example usability improvements



Common Weakness Enumeration
A community-developed list of SW & HW weaknesses that can become vulnerabilities
Top 25
Top HW CWE
New to CWE?
Start here!
Home > CWE List > CWE- Individual Dictionary Definition (4.14)
ID Lookup:
Go
Home
About ▼
CWE List ▼
Mapping ▼
Top-N Lists ▼
Community ▼
News ▼
Search
View customized information:
Conceptual
Operational
Mapping Friendly
Complete
Custom

CWE-416: Use After Free

Weakness ID: 416
Vulnerability Mapping: ALLOWED
Abstraction: Variant

▼ Description

Referencing memory after it has been freed can cause a program to crash, use unexpected values, or execute code.

▼ Extended Description

The use of previously-freed memory can have any number of adverse consequences, ranging from the corruption of valid data to the execution of arbitrary code, depe timing of the flaw. The simplest way data corruption may occur involves the system's reuse of the freed memory. Use-after-free errors have two common and sometin

- Error conditions and other exceptional circumstances.
- Confusion over which part of the program is responsible for freeing the memory.

In this scenario, the memory in question is allocated to another pointer validly at some point after it has been freed. The original pointer to the freed memory is used within the new allocation. As the data is changed, it corrupts the validly used memory; this induces undefined behavior in the process.

If the newly allocated data happens to hold a class, in C++ for example, various function pointers may be scattered within the heap data. If one of these function poi address to valid shellcode, execution of arbitrary code can be achieved.

▼ Alternate Terms

Dangling pointer

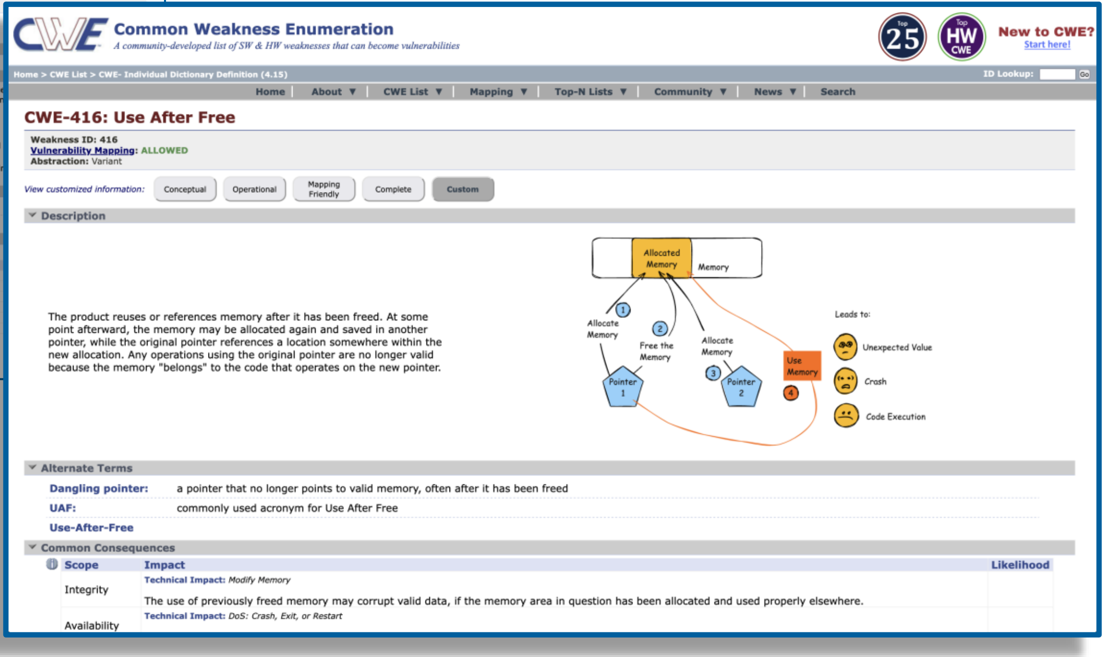
Use-After-Free

▼ Relationships

▼ *Relevant to the view "Research Concepts" (CWE-1000)*

Nature	Type	ID	Name
ChildOf	B	825	Expired Pointer Dereference
PeerOf	V	415	Double Free
CanFollow	B	364	Signal Handler Race Condition
CanFollow	B	1265	Unintended Reentrant Invocation of Non-reentrant Code Via Nested Calls
CanPrecede	B	120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
CanPrecede	B	123	Write-what-where Condition

▶ *Relevant to the view "Weaknesses for Simplified Mapping of Published Vulnerabilities" (CWE-1003)*
▶ *Relevant to the view "CISQ Quality Measures (2020)" (CWE-1305)*
▶ *Relevant to the view "CISQ Data Protection Measures" (CWE-1340)*



CWE-416: Use After Free

Weakness ID: 416
Vulnerability Mapping: ALLOWED
Abstraction: Variant

▼ Description

The product reuses or references memory after it has been freed. At some point afterward, the memory may be allocated again and saved in another pointer, while the original pointer references a location somewhere within the new allocation. Any operations using the original pointer are no longer valid because the memory "belongs" to the code that operates on the new pointer.

▼ Alternate Terms

Dangling pointer:	a pointer that no longer points to valid memory, often after it has been freed
UAF:	commonly used acronym for Use After Free
Use-After-Free	

▼ Common Consequences

Scope	Impact	Likelihood
Integrity	**Technical Impact:** *Modify Memory* The use of previously freed memory may corrupt valid data, if the memory area in question has been allocated and used properly elsewhere.	
Availability	**Technical Impact:** *DoS: Crash, Exit, or Restart*	

- **Changes:**
  - Concise summary of weakness with a visual aid
  - Reordering of elements to prioritize name, description, alternate terms, consequences, and mitigations

Summary

- These changes have been applied to a select number of entries in 4.15
  - https://cwe.mitre.org/news/archives/news2024.html#july16_CWE_Version_4.15_Now_Available
- In the June HW SIG meeting some members expressed interest in these usability updates to be applied to HW CWEs.
- Is this still a desire?
- If so which entries, should we target? A suggestion floated was to target some of the Most Important Hardware Weaknesses list.
- We would need help generating images. Looking for volunteers.

Next Meeting (Sep 13)

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