CVSS SIG Past, Present & Future

Current events with the FIRST CVSS SIG

Nick Leali, FIRST CVSS SIG Co-Chair
March 25, 2024
Agenda

1. Introduction
2. History
3. Current SIG Business
4. Future Plans
5. Resources
whoami – Nick Leali
Develop and document CVSS

Representation of a vulnerability’s severity

Common Vulnerability Scoring System (CVSS)

The Vulnerability Assessment Ecosystem

**CVSS**
- Severity of a vulnerability
- Zero to ten scale
- Captures the potential impact

**EPSS**
- Probability of exploitation
- 0% to 100% scale
- Guides focus of response efforts

**SSVC**
- Prioritize handling of a vulnerability
- Qualitative assessment of required response
- Takes into account the specific organization’s needs
What is new with CVSS v4.0?
CVSS v4.0 Recent History

- **8 June 2023**: Request for Public Comment
- **31 July 2023**: Closing of Public Comment
- **30 Sep. 2023**: Comment Responses Complete
- **1 Nov. 2023**: CVSS v4.0 Official Publication
- **1 Jan 2024**: First v4.0 Scores Published
Public Comment Period
### Public Comment Period

**Pros and Cons**

<table>
<thead>
<tr>
<th>Positive Aspects</th>
<th>Negative Aspects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Officially Reviewed</td>
<td>Time Consuming</td>
</tr>
<tr>
<td>Error Corrections</td>
<td>Mildly Ego Bruising</td>
</tr>
<tr>
<td>FAQ Document</td>
<td>No Massive Adjustments</td>
</tr>
<tr>
<td>Tooling Development</td>
<td>Must respond to each comment</td>
</tr>
</tbody>
</table>
CVSS
Presently
You are here
SIG Growth and Change

• New Members
• Providers and Consumers
• More diverse voices

• A Changing Conversation
  • Increased Focus on Usability
  • “Affordable Security”
  • Supply Chain
  • Making CVSS Easier
CVSS SIG Current Business

The Topics of Today
CVSS Adoption

Awareness

Chicken and egg problem
- Vendors to provide scores
- Customer need to provide them

Planned organizational adoption
- A few other public commitments

Are you and how long will you include v3.x scores?
- Current providers have both
- Can or should we coordinate around this?
CVSS Adoption

Part 2: Tooling

**Calculator work**
- Calculation is not simple algebra

**CVSS helper libraries**
- Review ongoing
- Post on FIRST.org

**Data sources**
- Updates soon

**Vulnerability Management platforms**
- Vendor outreach
CVSS Adoption

Part 2: Ease of Use

- CVSS in general is hard
- Requires mature program
- How can we ease adoption?
- How can we socialize the standard in general?
Documentation Updates

Examples
• Continued updating and evolution
• Taking requests
• Help wanted

FAQ
• Update as necessary
• Much of this came from the public comment period

User Guide
The Standard
Guidance

How vendors are thinking about subsequent system
- Known unknowns
- Reasonable best guess
- Avoid altogether

Supplemental metrics
- Some or all

How can we help consumers with threat and environmental metrics?
- Are organizations considering implementation plans
Future of CVSS

Near future, drive adoption and ease of use.

Further out, think about standard revision.
Future of CVSS

• Ease of Use
  • Complexity, relating to adoption
  • Documentation Updates
  • Socializing CVSS benefits
• V4.1
  • Attack Complexity weakness
  • User Interaction clarification

• V5.0
  • The Math
  • Reachability
  • Automatable expansion
  • Exploit Maturity expansion
  • New Supplemental Metrics
  • And more
The Math

➢ Discussions around refining the numeric scores.
➢ Is the number important?

*Stated problems:*
➢ Broad concerns about change
➢ Further distinguish scores
  ➢ Some metrics feel less important
➢ Crossing qualitative boundaries
  ➢ Some outliers
Questions?

Thank you!
Additional Resources

- **CVSS v4.0 Training**
  - [https://learn.first.org/catalog/info/id:126, cms_featured_course:1](https://learn.first.org/catalog/info/id:126, cms_featured_course:1)

- **CVSS Feedback**
  - cvss@first.org

- **CVSS Tooling**
  - [https://github.com/FIRSTdotorg/cvss-v4-calculator](https://github.com/FIRSTdotorg/cvss-v4-calculator)

- **CVSS v4.0 Site**
  - [https://www.first.org/cvss/v4/](https://www.first.org/cvss/v4/)

- **CVSS Documents**
  - [https://www.first.org/cvss/v4.0/specificiation-document](https://www.first.org/cvss/v4.0/specificiation-document)
  - [https://www.first.org/cvss/calculator/4.0](https://www.first.org/cvss/calculator/4.0)
  - [https://www.first.org/cvss/v4.0/user-guide](https://www.first.org/cvss/v4.0/user-guide)
  - [https://www.first.org/cvss/v4.0/examples](https://www.first.org/cvss/v4.0/examples)