Common Vulnerability Scoring System

The State of CVSS to Come

Dave Dugal

Dale Rich

Co-chairs of CVSS Special Interest Group

Agenda

- Current Status of CVSS v3.1
- Highlights: Approved and Proposed CVSS v4.0 Work Items
- CVSS v4.0 Timeline
- How to Get Involved
- Open Q&A

Current Status of CVSS

- CVSS v3.1 published in June 2019
- Improves upon v3.0 without introducing new metrics or values
  - *Allows for frictionless adoption of the new standard*
- Usability was a prime consideration
  - *Improve the clarity of concepts introduced in CVSS v3.0*
  - *Improve the overall ease of use of the standard*
  - *Clarify definitions with better explanations of existing base metrics*
  - *Lots and lots of examples of “Scope” described in Section 3.5 of the User Guide*
- Defined the CVSS Extensions Framework
- CVSS Glossary of Terms expanded and refined

Where we’ve been and where we’re going

- CVSS v3.x – Objectives
  - *The challenges of virtualization (Scope)*
  - *Increased objectivity and repeatability*
  - *Removed the “middle 90%” (Partial) Impact issue*
- CVSS v4.0 – Looking Forward
  - *Importance of using Threat Intelligence and Environmental metrics for accurate scoring*
  - *Operational Technology/Safety Metrics*
  - *Supplemental Concepts of “Automatable”, “Recovery” and “Mitigation Effort”*
  - *Representation of vendor-supplied Severity/Impact scoring within CVSS standard*
  - *Active vs. Passive “User Interaction”*
  - *“Attack Complexity” vs. “Attack Requirements”*
  - *Nomenclature*

CVSS v4.0: Approved Proposals

- Temporal Metric Group replaced with Threat Metric Group
- Remediation Level (RL) and Report Confidence (RC) Metrics removed
- Exploit Code Maturity updated to Exploit Maturity (E)
- Attack Requirements (AR) added as Base Metric
- Scope Metric expanded to tri-state value:
  - Unchanged / VulnerableComponent / ImpactedComponent
- Explicit Nomenclature added to specification: CVSS-BTE
- New Supplemental Metric Group
- Enhanced User Interaction Granularity (None/Active/Passive)
- Supplemental Metric: Automatable
- Repudiation Clarification for Integrity

CVSS v4.0: Proposed Work Items

- Supplemental Metric: Recovery
- Supplemental Metric: Mitigation Effort
- Supplemental Metric: Provider-Specific Urgency
- Kinetic (Safety) Impact Metric(s)
- Additional Threat Metrics
- Publish Risk Analysis Best Current Practices Addendum
- Support for Undefined (X) Base Metric Values?
- Additional Scope Clarification?
- Return of Target Distribution?

Check out https://bit.ly/cvssv4-workitems for complete list

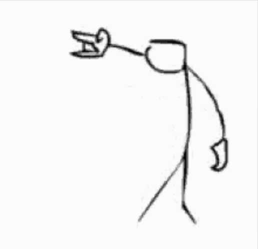
CVSS v4.0 Timeline

Work on CVSS v4.0 started in parallel with the publication of CVSS v3.1.

- 2017-12-08: Attack Requirements added as Base Metric in CVSS v4.0
- 2019-06-15: FIRST Board approves publication of CVSS v3.1
- 2020-02-20: Temporal Metric Group repurposed as Threat Metric Group
- 2020-04-20: Removal of Remediation Level and Report Confidence
- 2020-06-11: Update Scope metric to provide context to Impact Metrics
- 2020-07-02: Adoption of “Technical Severity” definition
- 2020-08-20: Exploit Maturity (E) Threat Metric and language
- 2020-09-10: CVSS-BTE Nomenclature adoption
- 2020-11-25: Addition of Supplemental Metric Group
- 2021-03-14: Repudiation explicitly added to definition of Integrity
- 2021-04-08: Expand User Interaction Granularity
- 2021-04-14: Addition of Automatable Supplemental Metric

Get Involved!

- The CVSS SIG holds weekly conference calls to discuss improvements to the standard
  - ❑ *Meetings to discuss CVSS v4.0 occur on Thursday at 13:00 ET*
- Become an active Participant in the meetings, or just join our mailing list as an Observer
- Details of how to get involved are on the CVSS home page: https://www.first.org/cvss
- Or rock it old school, and drop us an e-mail: cvss@first.org



Q
A