Announcing CVSS v4.0

Dave Dugal (Juniper Networks, USA)

Dale Rich (Black & Veatch, USA)

TLP: CLEAR

Overview of What's New in CVSS v4.0

- Finer granularity in Base Metrics
  - ➢ Attack Requirements (AT) added as Base Metric
  - ➢ Enhanced User Interaction Granularity (None/Active/Passive)
- Removal of downstream scoring ambiguity (read: Scope)
  - ➢ C/I/A expanded into separate Vulnerable System C/I/A and Subsequent System C/I/A
- Simplification of Threat metrics and improved scoring impact
  - ➢ Remediation Level, Report Confidence, and Exploit Code Maturity simplified to Exploit Maturity
- Supplemental attributes for vulnerability response
  - ➢ Supplemental Metric: Automatable
  - ➢ Supplemental Metric: Recovery
  - ➢ Supplemental Metric: Value Density
  - ➢ Supplemental Metric: Vulnerability Response Effort
  - ➢ Supplemental Metric: Provider Urgency
- Additional applicability to OT/ICS/IoT
  - ➢ Safety Metric Values added to Environmental Metrics

Technical Severity vs. Risk

CVSS Base scores (CVSS-B) represent “Technical Severity”

- Only takes into consideration the attributes of the vulnerability itself
- It is not recommended to use this alone to determine remediation priority

“Risk” is often a religious topic… but…

- CVSS-BTE scores take into consideration the attributes of the…
  - Base Score
  - Threat associated with the vulnerability
  - Environmental controls / Criticality

If used properly, CVSS-BTE scores represent more comprehensive attributes than many highly respected 3rd party security organizations consider when they generate their proprietary “Risk” ratings.

CVSS and EPSS and SSVC

Additional scoring systems have been recently introduced and adopted to handle complimentary aspects of vulnerability assessment and patch priority. These are welcome additions to the vulnerability scoring toolbox, providing innovative exploit prediction and decision support.

- **EPSS**: Exploit Prediction Scoring System

  A data-driven effort for estimating the likelihood (probability) that a software vulnerability will be exploited in the wild within 30 days.
  https://first.org/epss

- **SSVC**: Stakeholder-Specific Vulnerability Categorization

  A decision tree system for prioritizing actions during vulnerability management.
  https://cisa.gov/ssvc

Best Practices for Successful CVSS Usage

- Use databases and data feeds to automate the enrichment of your vulnerability data.
  - NVD (Base Metric Values)
  - Asset Management Database (Environmental Metric Values)
  - Threat Intelligence Data (Threat Metric Values)

- Find ways to view your vulnerability data based on important attributes
  - Support Teams Responsible for Resolution
  - Critical Applications
  - Internal vs. Externally facing
  - Business Units
  - Regulatory Requirements

CVSS v4.0 Schedule and Timeline 📅

- Request for Public Comment: June 8th, 2023 🎉
- Closing of Public Comment: July 31st, 2023
- Comment Responses Complete: August 31st, 2023
- CVSS v4.0 Official Publication: Q4/2023

Links to Docs, Specs, and Training

- CVSS SIG: https://first.org/cvss
- CVSS Online Training Course: https://www.first.org/cvss/training
- CVSS v4.0 Work In Progress: https://www.first.org/cvss/v4-0
- CVSS v4.0 Specification: https://www.first.org/cvss/v4-0/specification-document
- CVSS v4.0 User Guide: https://www.first.org/cvss/v4-0/user-guide
- CVSS v4.0 Calculator: https://www.first.org/cvss/calculator/v4-0