presented by

CVSSv4 Firmware Scoring

A Call For Collaborative Action

UEFI Fall 2023 Developers Conference & Plugfest

October 9-12, 2023

Presented by Dick Wilkins (Phoenix Technologies)

Agenda

- What is CVSS?
- Scoring Basics
- How has V4.0 Changed Things
- Demo
- Call to Action!
- Questions

What is CVSS?

- National Infrastructure Advisory Council (NIAC) launched CVSSv1 in February 2005. In April 2005, control of CVSS was handed to FIRST*
- It was "designed to provide open and universally standard severity ratings of software vulnerabilities"
  - CVSSv2 was released in June 2007
  - CVSSv3 was released in June 2015
  - CVSSv3.1 was released in June 2019
  - CVSSv4 scheduled for release in October 2023

* FIRST is the global Forum of Incident Response and Security Teams

Who Uses It?

CVSS has been adopted as the primary method for quantifying the severity of vulnerabilities by many of companies and organizations, including:

- The National Vulnerability Database (NVD)
- The Open-Source Vulnerability Database (OSVDB)
- US CERT/CC and many other national CERT teams and PSIRT groups

Scoring Variability with V3.1

Variability causes, per the study referenced below:

- CVSS metrics Attack Vector, User Interaction and Scope were not consistently assessed
- The CVSS documentation is rarely consulted, 30% of scorers have never read it

But:

While 85% of evaluators find CVSS inconsistent, most participants (80%) still find it a useful tool. Evaluator quote: *“CVSS is like democracy: the worst system available, except for all the other systems ever tried.”*

Ref: *Shedding Light on CVSS Scoring Inconsistencies: A User-Centric Study on Evaluating Widespread Security Vulnerabilities;* Julia Wunder, Andreas Kurtz, Christian Eichenmüller, Freya Gassmann, and Zinaida Benenson, To appear in the Proceedings of the IEEE Symposium on Security and Privacy (S&P) 2024

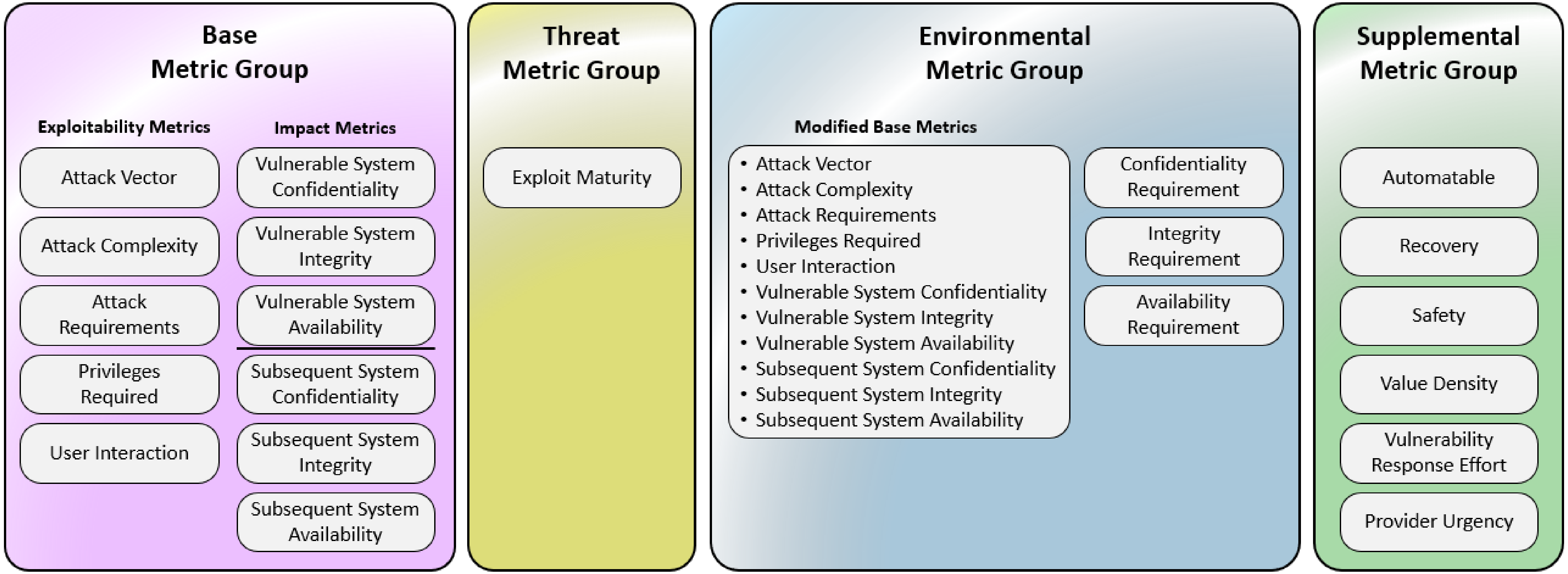
Alternatives to CVSS

- CVSS - Focuses on the innate characteristics of vulnerabilities culminating in a severity score (NOT risk to the user)
- SSVC - Prioritizes order of vulnerability remediation
- EPSS - Estimates the probability that a software vulnerability will be exploited in the wild

Major Changes in V4

- Scope Removed - The concept of Scope has been replaced with the concepts of:
  - Vulnerable system (VC, VI, VA), and
  - Subsequent system (SC, SI, SA),
  - capturing impacts from both, where relevant.
- The documentation and online learning tool have been improved, particularly for Attack Vector & User Interaction

CVSSv4 Metric Groups



Base Metric Group

Exploitability Metrics

- Attack Vector
- Attack Complexity
- Attack Requirements
- Privileges Required
- User Interaction

Impact Metrics

- Vulnerable System Confidentiality
- Vulnerable System Integrity
- Vulnerable System Availability
- Subsequent System Confidentiality
- Subsequent System Integrity
- Subsequent System Availability

Threat Metric Group

- Exploit Maturity

Environmental Metric Group

Modified Base Metrics

- Attack Vector
- Attack Complexity
- Attack Requirements
- Privileges Required
- User Interaction
- Vulnerable System Confidentiality
- Vulnerable System Integrity
- Vulnerable System Availability
- Subsequent System Confidentiality
- Subsequent System Integrity
- Subsequent System Availability

- Confidentiality Requirement
- Integrity Requirement
- Availability Requirement

Supplemental Metric Group

- Automatable
- Recovery
- Safety
- Value Density
- Vulnerability Response Effort
- Provider Urgency

Score Content Indicator

CVSS Nomenclature	CVSS Metrics Used
CVSS-B:V4.0	Base metrics
CVSS-BE:V4.0	Base and Environmental metrics
CVSS-BT:V4.0	Base and Threat metrics
CVSS-BTE:V4.0	Base, Threat, Environmental metrics

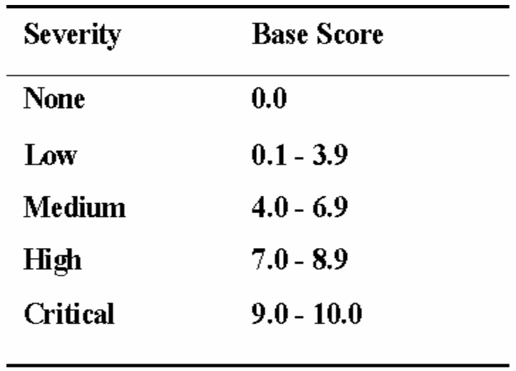
The addition of the –B, -BE, -BT, or -BTE indicates which metrics are included with a specific score

New Scoring System Development

In order to create a more understandable and defensible scoring tool, this process was used

1. Use metric groups to gather the 15 million CVE-BTE vectors into 271 equivalence sets
2. Solicit experts to compare vectors representing each equivalence set
3. Use the expert comparison data to calculate an order of vectors from least severe to most severe
4. Solicit expert opinion to decide what vector group in the ordering of vectors represents the boundary between qualitative severity scores to be backwards compatible with qualitative severity score boundaries from CVSS v3.x.

New Scoring System, Cont.



Severity	Base Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

5. Compress the vector groups in each qualitative severity bin into the number of available scores in that bin (for example, 9.0 to 10.0 for critical, 7.0 to 8.9 for high, etc.)
6. Create a small score modification factor that adjusts the scores of vectors within a vector group so that a change of any metric value results in a score change. The intent is that the score change is not larger than the uncertainty in the ranking of the vector groups as collected from the expert comparison data in step 2.

Demo

- Link to the CVSSv4 online calculator

https://www.first.org/cvss/calculator/4.0

CVSS V4.0 Links

- https://www.first.org/cvss/v4.0/specification-document
- https://www.first.org/cvss/v4.0/user-guide
- https://www.first.org/cvss/v4.0/examples
- https://Learning.first.org Online learning on scoring
- https://www.first.org/cvss/calculator/4.0

What we all should be doing

Calls to Action!

Scoring is Not Always Simple

- Phoenix provided firmware scoring examples for CVSSv3.1
- These have been carried forward in the V4.0 examples document
  - Lenovo ThnkPwn Exploit (CVE-2016-5729)
  - Failure to Lock Flash on Resume from sleep (CVE-2015-2890)
  - Intel DCI Issue (CVE-2018-3652)
- **Others are invited to provide good firmware scoring examples**

CNA Recommendation

- CVSS vector/score is part of a CVE record in the NVD
- A CNA (CVE Numbering Authority) can:
  - Assign their own CVE numbers on demand
  - Control the content of their CVE reports
  - Control the date the information becomes public
- About 50% of UEFI Promoter/Contributors are CNAs
- **If you handle more than one or two vulnerabilities per year, you should become a CNA**
- https://www.cve.org/ProgramOrganization/CNAs

CVSS Scoring Consistency

- CVSS Scoring can be hard, particularly with firmware vulnerabilities
- Most scoring info and examples target networks, software and cloud
- Consistency between scorers is difficult
- **Can we find a way for the firmware community to work together for more consistency in scores of FW vulnerabilities?**

Discussion?   Questions?

Thanks for attending the UEFI Fall 2023 Developers Conference & Plugfest

For more information on UEFI Forum and UEFI Specifications, visit http://www.uefi.org

presented by

phoenix® technologies