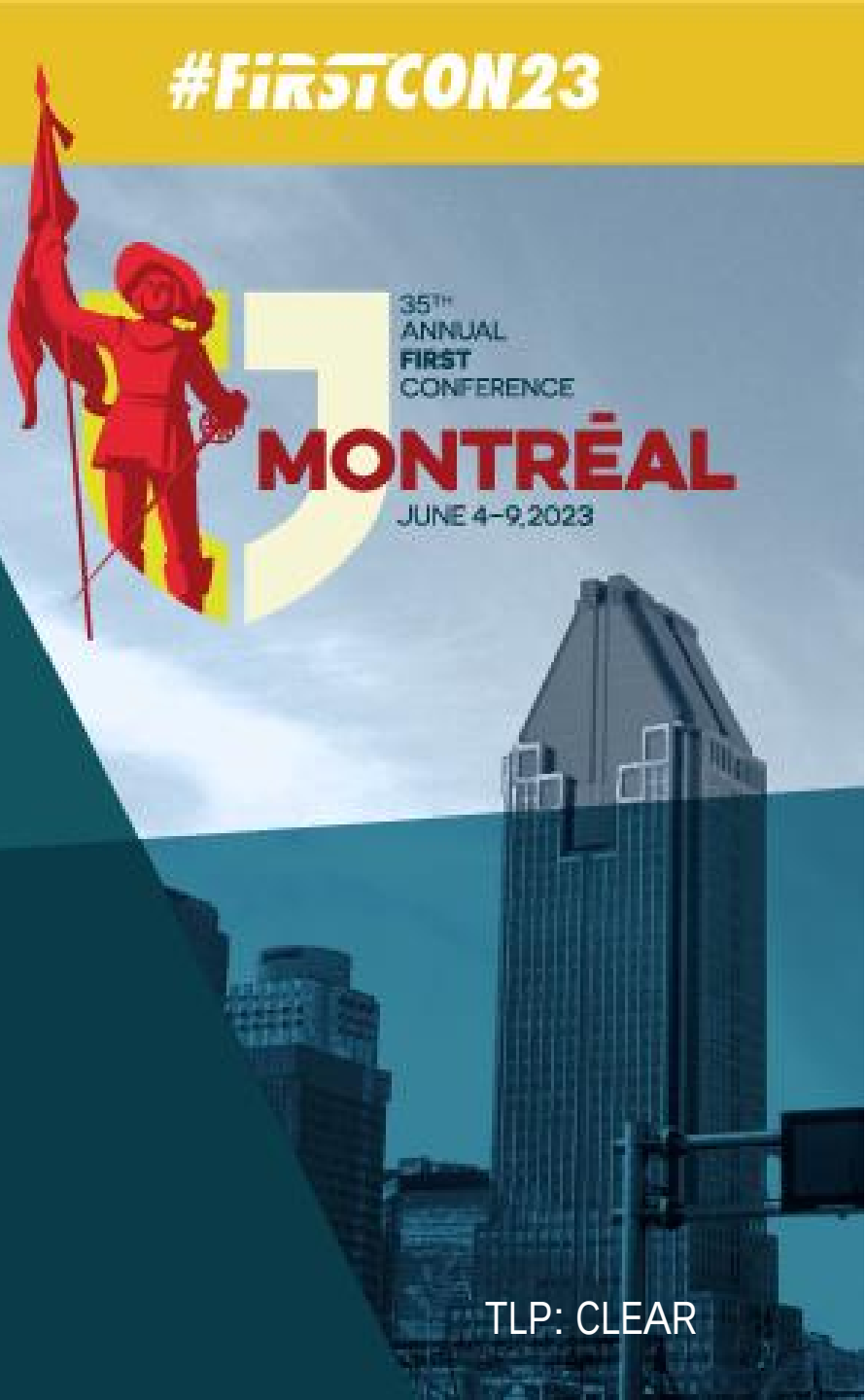
Announcing CVSS v4.0



Dave Dugal (Juniper Networks, USA)
Dale Rich (Black & Veatch, USA)

TLP: CLEAR

about.me

- dave@juniper.net
- @vipergeek@infosec.exchange
- @JuniperSIRT
- keybase.io/ViperGeek
- about.me/ViperGeek

Dave Dugal
Principal Product Security Incident Manager
Juniper SIRT

- 1980s: Digital Equipment Corporation
  - Mini-computers ruled
- 1990s: Bay Networks/Nortel
  - Who remembers circuit-switched networks? Anyone?
- 21st Century: Juniper Networks
  - Packet-pusher Tech Support, then Product Security Incident Response Team
- 2017-Present: CVSS-SIG Co-Chair

CVSS v4.0: Agenda

- Introduction to the Common Vulnerability Scoring System
- Challenges and Opportunities Identified in CVSS v3.1
- High-Level Goals of CVSS v4.0
  - Finer granularity
  - Removal of downstream scoring ambiguity (read: Scope)
  - Simplification of Threat metrics and improved scoring impact
  - Supplemental attributes for vulnerability response
  - Additional applicability to OT/ICS/IoT
- Meet the New CVSS v4.0 Calculator

CVSS v4.0 Agenda (cont.)

- Technical Severity vs. Risk
- Contrast and Compare CVSS with EPSS and SSVC
- Highlight best current practices for correct usage of CVSS, including documentation, and training
- CVSS is not just the Base score (CVSS-BTE)
- CVSS v4.0 Public Preview 

CVSS Chronology

- Prehistoric Times (pre-2005)
  - Vendors used custom, incompatible rating systems to define severity
  - NIAC recognized a need to standardize vulnerability measurements across software and platforms
- February 2005: CVSS version 1
  - CVSS v1 was developed by a handful of “pioneers” with the aim of reaching wide industry adoption.
  - Received little peer review before its release, and much criticism after its release
  - Ambiguities in the metric definition made scoring and score interpretation hard.
  - In April 2005, NIAC selected the Forum of Incident Response and Security Teams (FIRST) to become the custodian of CVSS for future development.

CVSS Chronology (cont.)

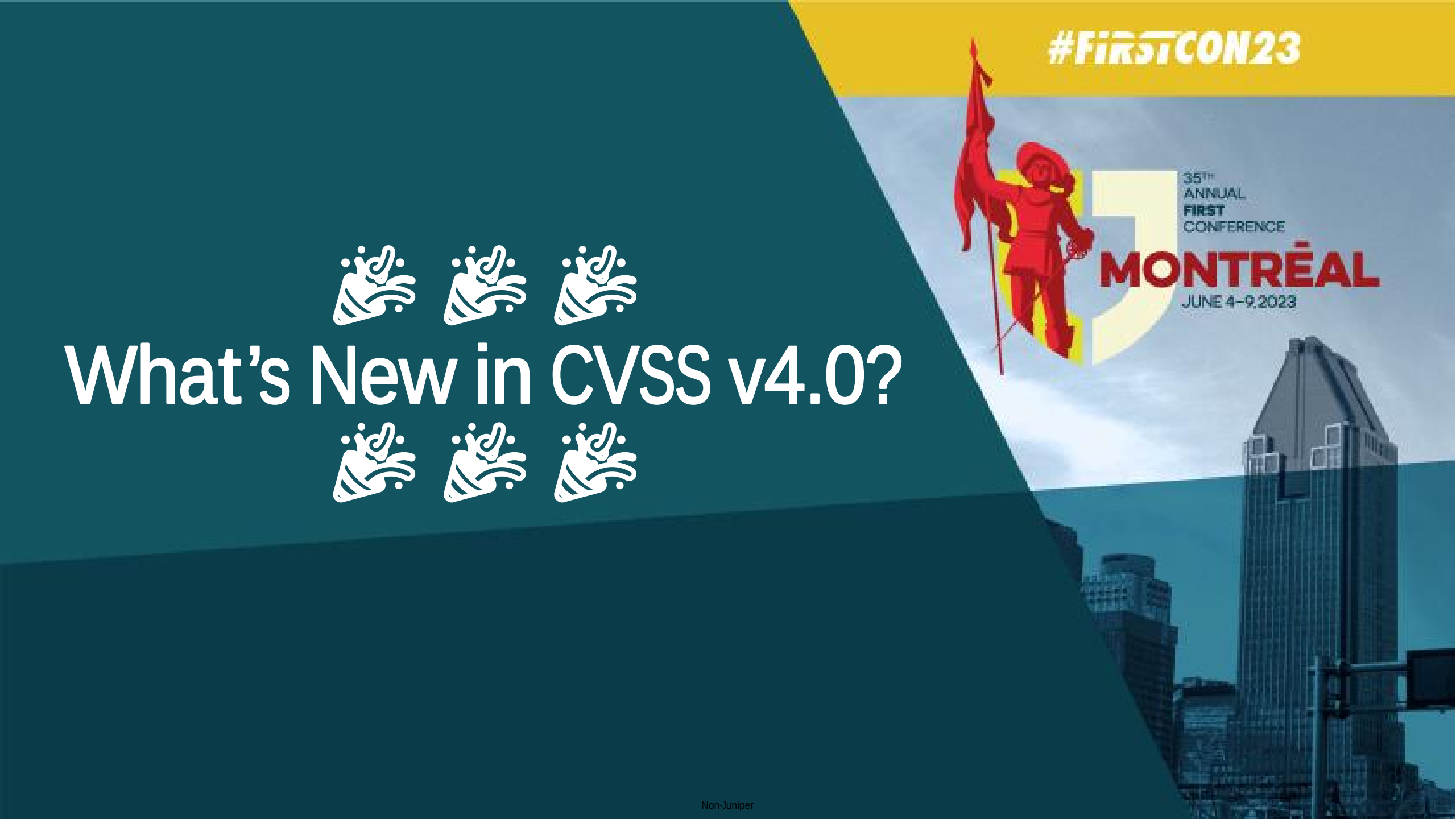
- June 2007: CVSS version 2
  - Over a dozen members of the CVSS-SIG collaborated extensively through 2006 and 2007 to revise and improve CVSS v1 by testing and re-testing hundreds of real-world vulnerabilities.
  - Reduced inconsistencies, provides additional granularity, and more accurately reflected the wide variety of vulnerabilities (at the time).
- June 2015: CVSS version 3.0
  - Introduced the concept of “Scope” to handle the scoring of vulnerabilities that exist in one software component, but impact a separate software, hardware, or networking component.
  - Also updated terms (Access → Attack), added Privileges Required, and resolved the “middle 90%” issue of Partial impact by introducing Low/High.

CVSS Chronology (cont.)

- June 2019: CVSS version 3.1
  - Clarified and improved upon version 3.0 without introducing new metrics or values
  - Improved upon clarity of concepts to improve the overall ease of use of the standard
  - Added the CVSS Extensions Framework and updated Glossary of Terms
  - *CVSS is designed to measure the severity of a vulnerability and should not be used alone to assess risk.*
- 2022: CVSS version 4.0
  - Importance of using Threat Intelligence and Environmental metrics for accurate scoring
  - Operational Technology/Safety Metrics
  - Supplemental Concepts of “Automatable”, “Recovery” and “Vulnerability Response Effort”
  - Representation of provider-supplied Urgency within CVSS standard
  - Active vs. Passive “User Interaction”
  - “Attack Complexity” vs. “Attack Requirements”
  - Nomenclature

Challenges and Critique of CVSS 3.1

- CVSS Base Score being used as primary input to risk analysis
- Not enough real time threat and supplemental impact details represented
- Only applicable to I.T. systems
- Health, human safety, and industrial control systems not well represented
- Scores published by vendors are often High or Critical (7.0+)
- Insufficient granularity – fewer than 99 discrete CVSS scores in practice
- Temporal Metrics do not effectively impact the final CVSS score
- The math seems overly complicated and counterintuitive
- Where did you come up with that wacky formula???



What's New in CVSS v4.0?

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

Nomenclature

As we all know, CVSS is not just the Base Score.

To stress this idea, new nomenclature has been adopted:

- CVSS-B: CVSS Base Score
- CVSS-BT: CVSS Base + Threat Score
- CVSS-BE: CVSS Base + Environmental Score
- CVSS-BTE: CVSS Base + Threat + Environmental Score

New Base Metric: Attack Requirements

Problem: The “low” and “high” AC values do not reflect the significant differences between conditions currently compressed in the definition of “high” complexity. For example, the evasion of security mitigation techniques such as ASLR or crypto objectively require significantly higher exploit complexity than iterating an attack to win a race condition; yet both conditions currently result in the same “penalty” to the final severity score.

This proposal aims at addressing this by splitting the current AC definition in two metrics, called “Attack Complexity” (AC) and “Attack Requirements” (AT) that respectively convey the following:

Attack Complexity - Reflect the exploit engineering complexity required to evade or circumvent defensive or security-enhancing technologies. (defensive measures)

Attack Requirements - Reflect the prerequisite conditions of the vulnerable component that make the attack possible.

Updated Base Metric: User Interaction

The intention of this proposal is to allow for additional granularity when considering the interaction of a user with a vulnerable component, and details are as follows:

None (N):	The vulnerable system can be exploited **without interaction** from any human user, other than the attacker.
Passive (P):	Successful exploitation of this vulnerability requires **limited interaction** by the targeted user with the vulnerable component and the attacker's payload. These interactions would be considered involuntary and do not require that the user actively subvert protections built into the vulnerable component.
Active (A):	Successful exploitation of this vulnerability requires a **targeted user to perform specific, conscious interactions** with the vulnerable component and the attacker's payload, or the user's interactions would actively subvert protection mechanisms which would lead to exploitation of the vulnerability

Retired Base Metric: Scope

Scope may have been the least loved and least understood CVSS metric ever.

- Caused inconsistent scoring between product providers
- Implied “lossy compression” of impacts of vulnerable and impacted systems

- **Solution:** Impact Metrics expanded into two sets:

✓ Vulnerable System Confidentiality (VC), Integrity (VI), Availability (VA)
✓ Subsequent System(s) Confidentiality (SC), Integrity (SI), Availability (SA)

“Modified” Environmental Metrics updated accordingly

Temporal → Threat Metric Group

- Remediation Level (usually O) and Report Confidence (usually C) retired
- Exploit *Code* Maturity renamed Exploit Maturity
- Enhanced impact for Threat Metric values

Adjusts “reasonable worst case” Base score by using threat intelligence to reduce the CVSS-BTE score, addressing concerns that many CVSS (Base) scores are too high.

New Metric Group: Supplemental Metrics Group

Supplemental Metrics provide the ability to define new metrics that describe and measure **additional extrinsic attributes** of a vulnerability.

The **information consumer** can then use the values of these Supplemental Metrics to take additional actions if they so choose, applying locally significant importance to the metrics and values.

No metric will define numerical impact on the final calculated CVSS score (e.g., CVSS-BTE). Organizations may then assign importance and/or effective impact of each metric, or set/combination of metrics, giving them more, less, or absolutely no effect on the final risk analysis. Metrics and values will simply convey additional extrinsic characteristics of the vulnerability itself.

Note: All Supplemental Metrics supplied by the information provider are **optional**.

New Focus on OT: Safety Metrics and Values

Many vulnerabilities today have impacts outside of the traditional C/I/A triad of logical impacts. Increasingly more common is a concern that, while logical impacts may or may not be recognized on a vulnerable or impacted system, it is possible for tangible harm to occur to humans as a result of a vulnerability exploit.

IoT, ICS and healthcare sectors in particular care greatly about being able to identify this kind of impact as part of the CVSS specification to help drive prioritization of issues aligned with their growing concerns.

OT: Consumer Supplied Environmental **Safety**

When a system **does not** have an intended use or fitness of purpose aligned directly to safety but may have safety implications as a matter of how or where it is deployed, it is possible that exploiting a vulnerability within that system may have safety impact(s) which can be represented in the Environmental Metrics group.

The Safety metric value measures the impact regarding the Safety of a human actor or participant that can be predictably injured as a result of the vulnerability being exploited. Unlike other impact metric values, Safety can only be associated to the Subsequent System(s) impact set and should be considered in addition to the N/L/H impact values for Availability and Integrity metrics.

OT: Consumer Supplied Environmental **Safety**

- Modified Integrity of Subsequent System: Safety (MSI:S)

Successful exploitation compromises the integrity of the vulnerable system (such as changing the dosage for a medication infusion pump), resulting in an impact to human health and safety (injury).

- Modified Availability of Subsequent System: Safety (MSA: S)

Successful exploitation compromises the availability of the vulnerable system (such as a brake system in a car becoming unavailable), resulting in an impact to human health and safety (injury).

OT: Provider Supplied Supplemental Safety

When a system **does** have an intended use or fitness of purpose aligned to safety, it is possible that exploiting a vulnerability within that system may have Safety impact which can be represented in the Supplemental Metrics group.

The possible values for the Safety Supplemental Metric are as follows:

Present (P):	Consequences of the vulnerability meet definition of IEC 61508 consequence categories of "marginal," "critical," or "catastrophic."
Negligible (N):	Consequences of the vulnerability meet definition of IEC 61508 consequence category "negligible."
Not Defined (X):	The value of this metric has not been defined for this vulnerability.

Note: Providers are not ***required*** to supply Supplemental Metrics. They can be supplied as needed, based solely on what the provider choses to convey on a case-by-case basis.

The Supplemental Metrics

Supplemental Metric: Automatable

The “Automatable” metric captures the answer to the question ”Can an attacker automate exploitation of this vulnerability across multiple targets?” based on steps 1-4 of the kill chain: reconnaissance, weaponization, delivery, and exploitation.

No	Attackers cannot reliably automate all steps of the kill chain for this vulnerability (reconnaissance, weaponization, delivery, and exploitation).	1. the vulnerable component is not searchable or enumerable, 2. weaponization requires human direction for each target, 3. delivery uses channels that network security configurations block 4. exploitation is not reliable, due to exploit-prevention techniques enabled by default
Yes	Attackers can reliably automate all steps of the kill chain (reconnaissance, weaponization, delivery, and exploitation).	As one heuristic for yes, if the vulnerability allows unauthenticated remote code execution or command injection, the expected response is yes. Analysts should provide an argument or demonstration that all four steps are able to be automated rather than solely relying on heuristics.

Supplemental Metric: Recovery

This metric describes the resilience of a Component/System to recover services, in terms of performance and availability, after an attack has been performed.

Automatic (A)	The Component/System recovers automatically after an attack.
User (U)	The Component/System requires manual intervention by the user to recover services, after an attack.
Irrecoverable (I)	The Component/System is irrecoverable by the user, after an attack.

Supplemental Metric: Value Density

Value Density describes the resources that the attacker will gain control over with a single exploitation event. It has two possible values, diffuse and concentrated.

Diffuse	The system that contains the vulnerable component has limited resources. That is, the resources that the attacker will gain control over with a single exploitation event are relatively small.
Concentrated	The system that contains the vulnerable component is rich in resources. Heuristically, such systems are often the direct responsibility of “system operators” rather than users.

Supplemental Metric: Vulnerability Response Effort

Provides supplemental information on how difficult it is for consumers to provide an initial response to the impact of vulnerabilities for deployed products and services in their infrastructure. The consumer can then take this additional information on effort required into consideration when applying mitigations and/or scheduling remediation.

Low (L)	The effort required to respond to a vulnerability is low/trivial.
Moderate (M)	The actions required to respond to a vulnerability require some effort on behalf of the consumer and could cause minimal service impact to implement.
High (H)	The actions required to respond to a vulnerability are significant and/or difficult, and may possibly lead to an extended, scheduled service impact. Alternately, response to the vulnerability in the field is not possible remotely. The only resolution to the vulnerability involves physical replacement.

Supplemental Metric: Provider Urgency

To facilitate a standardized method to incorporate additional provider-supplied assessment, an optional “pass-through” Supplemental Metric called Provider Urgency has been defined.

While any provider along the product supply chain may provide a Supplemental Urgency rating:

Library Maintainer → OS/Distro Maintainer → Provider 1 … **Provider n** (PPP) → Consumer

the Penultimate Product Provider (PPP) is best positioned to provide a direct assessment of Urgency.

Supplemental Metric: Provider Urgency

Provider Urgency Metric Values:

Red:	Provider has assessed the impact of this vulnerability as having the highest urgency
Amber:	Provider has assessed the impact of this vulnerability as having a moderate urgency
Green:	Provider has assessed the impact of this vulnerability as having a reduced urgency
Clear:	Provider has assessed the impact of this vulnerability as having low or no urgency (Informational)

CVSS v4.0: The Calculator

Base Metrics

Exploitability Metrics

Attack Vector (AV):	**Network (N)**	Adjacent (A)	Local (L)	Physical (P)
Attack Complexity (AC):	**Low (L)**	High (H)		
Attack Requirements (AT):	**None (N)**	Present (P)		
Privileges Required (PR):	**None (N)**	Low (L)	High (H)	
User Interaction (UI):	**None (N)**	Passive (P)	Active (A)	

Vulnerable System Impact Metrics

Confidentiality (VC):	High (H)	Low (L)	**None (N)**
Integrity (VI):	High (H)	Low (L)	**None (N)**
Availability (VA):	High (H)	Low (L)	**None (N)**

Subsequent System Impact Metrics

Confidentiality (SC):	High (H)	Low (L)	**None (N)**
Integrity (SI):	High (H)	Low (L)	**None (N)**
Availability (SA):	High (H)	Low (L)	**None (N)**

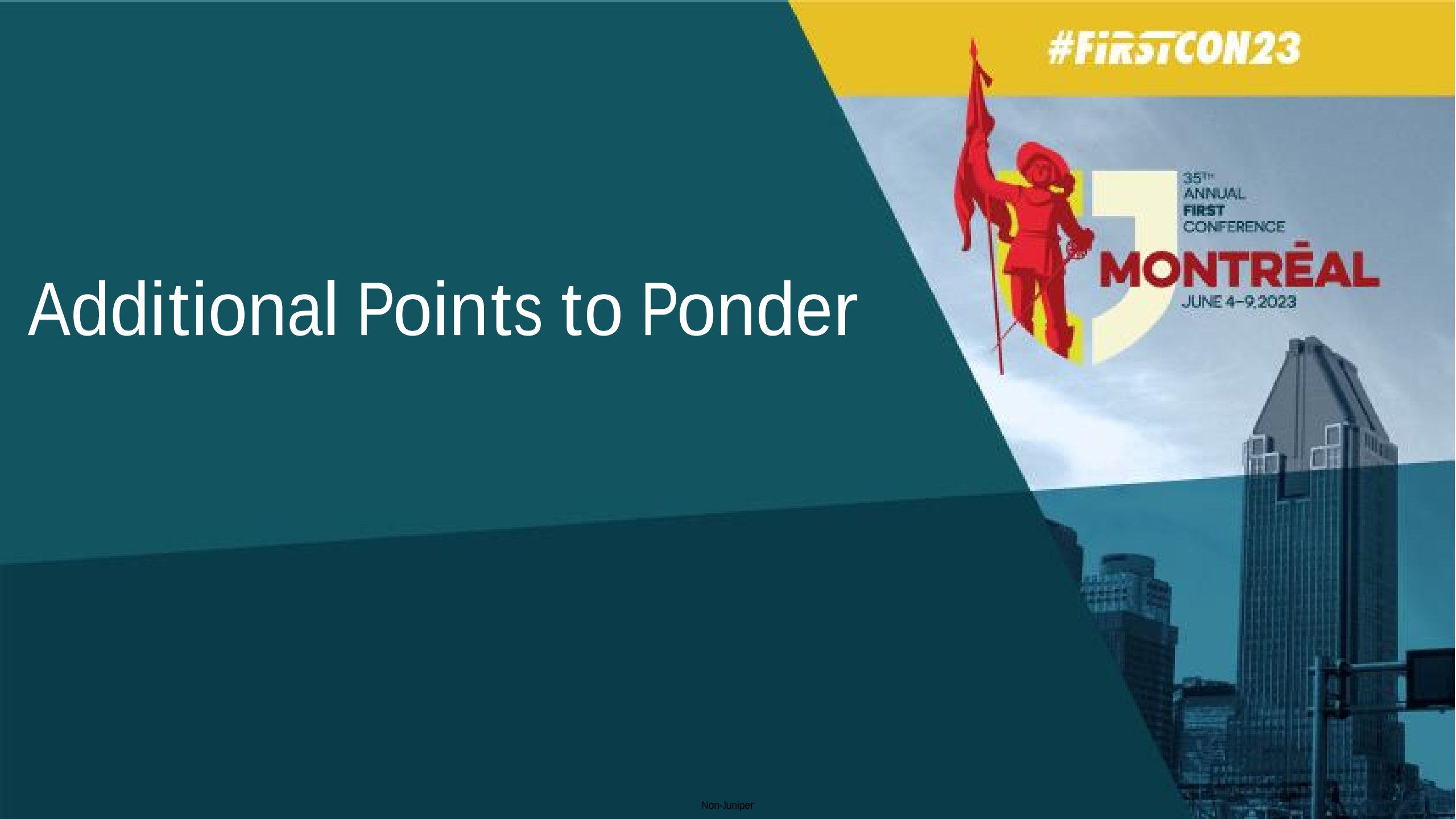
Supplemental Metrics

Safety (S):	**Not Defined (X)**	Negligible (N)	Present (P)		
Automatable (AU):	**Not Defined (X)**	No (N)	Yes (Y)		
Recovery (R):	**Not Defined (X)**	Automatic (A)	User (U)	Irrecoverable (I)	
Value Density (V):	**Not Defined (X)**	Diffuse (D)	Concentrated (C)		
Vulnerability Response Effort (RE):	**Not Defined (X)**	Low (L)	Moderate (M)	High (H)	
Provider Urgency (U):	**Not Defined (X)**	Clear	Green	Amber	Red

New and Novel Approach to Math

- Use metric groups to gather 15 million CVSS vectors into 271 equivalence sets
- Solicit expert opinion to compare vectors representing each equivalence set
- Calculate the order of vectors from least severe to most severe
- Determine boundaries between Qualitative Severity Ratings compatible with qualitative severity boundaries from CVSS v3.x.
- 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.)
- Leverage interpolation to adjust scores within a vector group to ensure changes in any metric value results in a score change.

Additional Points to Ponder



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: September 30th, 2023
- CVSS v4.0 Official Publication: Q4/2023 (est. October 31st, 2023)

Public comments, questions, and concerns: cvss@first.org

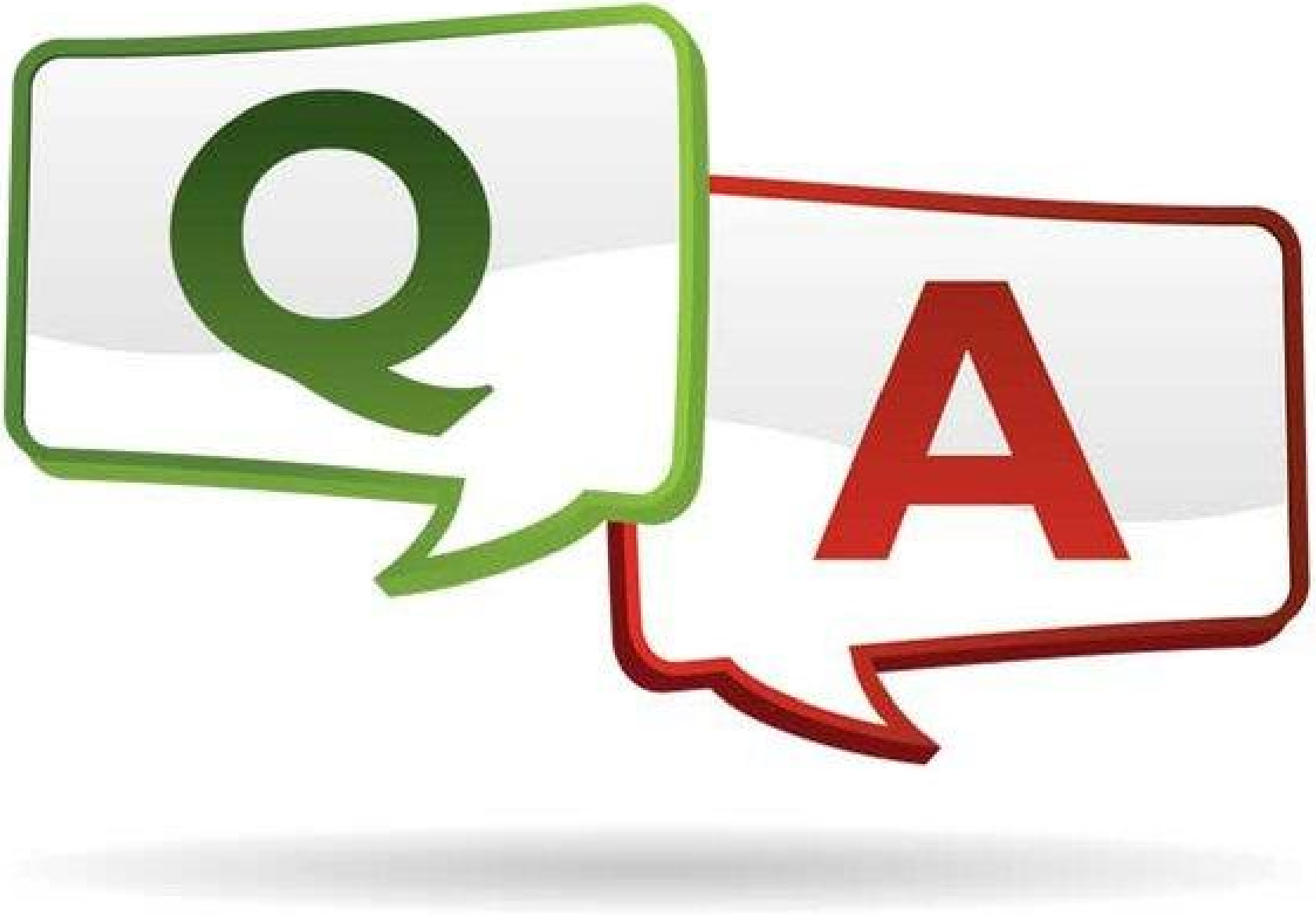
CVSS 4.0 Contributors and Participants

Abdulhamid Adebayo, IBM
Srividya Ananth, Peter Mell, Christopher Turner, NIST
Chandan BN, Palo Alto Networks
Feng Cao, Janane Suresh, Oracle
Francesco Casotto, Arkadeep Kundu, Nick Leali, Cisco
Matthew Coles, Phillip Nordwall, Dell Technologies
Khushali Dalal, Dave Dugal, Akshat Vaid, Juniper Networks
Giorgio Di Tizio, Fabio Massacci, University of Trento
Karan Dwivedi, Google
Ben Edwards, Cyentia
Troy Fridley, Acuity Brands
Jeff Heller, Sandia National Laboratories
Adrian Henrick
Allen Householder, CERT/CC
Miguel Hummel, Margaux Pagano, Citi
Fabrice Kah, Schneider Electric
Stav Kaufman, Skybox Security
Austin Kimbrell, Stanislav Kontar, Fábio Olivé Leite, Red Hat
Toby Kohlenberg
Jim Kohli, GE Healthcare
Milind Kulkarni, Ericsson
Angela Lindberg, SAP
Kumar Mangipudi
Bruce Monroe, Intel
Vivek Nair, Daniel Sommerfeld, Microsoft
Wilfried Pascault, CERT Orange Cyberdefense
Diana Prusova, Accenture Security
Marián Rehák
Dale Rich, Black & Veatch
Melinda Rosario
Jonathan Spring, CISA
Masato Tereada
Matt Tesauro
Richard Wilkins, Phoenix Technologies, Inc.

Special thanks to Grace Staley from CAPS, LLC. for her tireless work facilitating the CVSS SIG meetings

Links to Docs, Specs, and Training

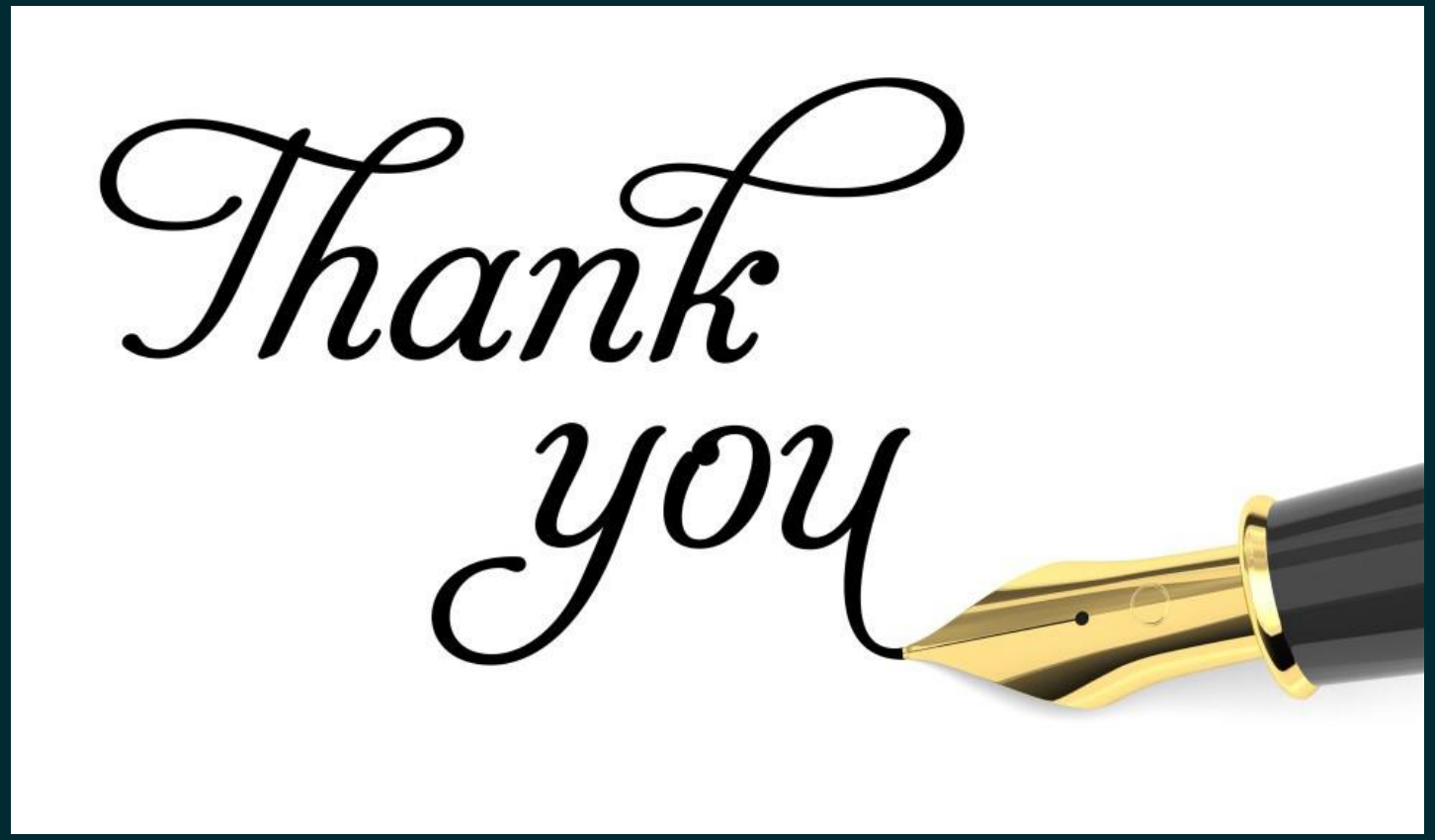
- CVSS SIG: https://first.org/cvss
- CVSS Online Training Course: https://www.first.org/cvss/training
- CVSS v4.0 Public Preview: https://www.first.org/cvss/v4-0
- CVSS v4.0 Specification: https://www.first.org/cvss/v4-0/specification-document
- CVSS v4.0 User Guide: https://www.first.org/cvss/v4-0/user-guide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


Q
A

Thank You!

#FIRSTCON23

35TH ANNUAL FIRST CONFERENCE
MONTRÉAL
JUNE 4-9,2023



Dave Dugal

- dave@juniper.net
- @vipergeek@infosec.exchange
- @JuniperSIRT
- keybase.io/ViperGeek
- about.me/ViperGeek