Here Comes CVSS v4.0

Dave Dugal (Juniper Networks)
Dale Rich (Black & Veatch)
ABOUT US

Dave Dugal
Principal Product Security Incident Manager
Juniper SIRT

Dale Rich
Cyber Security Operations Senior Manager
Black & Veatch
AGENDA

• Introduction
  o CVSS Chronology
  o Challenges of v3 and Goals of v4

• What’s New in CVSS v4?
• CVSS Best Practices
• Wrap-it-up
CVSS CHRONOLOGY

• Prehistoric Times (pre-2005)
  o Vendors used custom, incompatible rating systems to define severity
  o NIAC recognized a need to standardize vulnerability measurements across software and platforms
CVSS CHRONOLOGY

• February 2005: CVSS version 1
  o CVSS v1 was developed by a handful of “pioneers” with the aim of reaching wide industry adoption.
  o Received little peer review before its release, and much criticism after its release
  o Ambiguities in the metric definition made scoring and score interpretation hard.
  o 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

• June 2007: CVSS version 2
  o 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.
  o Reduced inconsistencies, provides additional granularity, and more accurately reflected the wide variety of vulnerabilities (at the time).
CVSS CHRONOLOGY

• June 2015: CVSS version 3.0
  o 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.
  o Also updated terms (Access → Attack), added Privileges Required, and resolved the “middle 90%” issue of Partial impact by introducing Low/High.
CVSS CHRONOLOGY

• 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.
CVSS CHRONOLOGY

• 2022: CVSS version 4.0
  o Importance of using Threat Intelligence and Environmental metrics for accurate scoring
  o Operational Technology/Safety Metrics
  o Supplemental Concepts of “Automatable”, “Recovery” and “Vulnerability Response Effort”
  o Representation of provider-supplied Urgency within CVSS standard
  o Active vs. Passive “User Interaction”
  o “Attack Complexity” vs. “Attack Requirements”
  o Nomenclature
CHALLENGES OF V3 AND GOALS OF V4

• CVSS Base Score being used as primary input to risk analysis
  o Not enough real time threat and supplemental impact details represented

• Only applicable to I.T. systems
  o 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
  o Where did you come up with that wacky formula???
AGENDA

• Introduction

• What’s New in CVSS v4?
  o Nomenclature
  o Finer Granularity
  o Removal of “Scope”
  o Simplification of Threat Metrics
  o Supplemental Attributes
  o OT Safety

• CVSS Best Practices

• Wrap-it-up
WHAT'S NEW – NOMENCLATURE

CVSS is not just the Base Score
To stress this concept, 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

The more metrics used to enrich your CVSS scoring, the higher quality your assessment will be.
WHAT’S NEW – FINER GRANULARITY

New Base Metric: Attack Requirements (AT)

• **Problem:** The “low” and “high” Attack Complexity (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.

• **Solution:** Splits the current AC definition in two metrics...
  - 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 (UI)

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:

<table>
<thead>
<tr>
<th>Metric Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (N)</td>
<td>The vulnerable system can be exploited without interaction from any human user, other than the attacker.</td>
</tr>
<tr>
<td>Passive (P)</td>
<td>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.</td>
</tr>
<tr>
<td>Active (A)</td>
<td>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</td>
</tr>
</tbody>
</table>
WHAT’S NEW – SCOPE IS RETIRED!

Retired Base Metric: SCOPE (S)

- **Problem**: 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)
WHAT’S NEW – SIMPLIFICATION OF THREAT METRICS

• “Temporal” metric group renamed to “Threat”
• Remediation Level (RL) is retired
• Report Confidence (RC) is retired
• “Exploit Code Maturity” renamed to “Exploit Maturity”
WHAT’S NEW – SUPPLEMENTAL METRIC 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.**
Supplemental Metrics

- Automatable
- Recovery
- Value Density
- Vulnerability Response Effort
- Provider Urgency
WHAT’S NEW – SUPPLEMENTAL METRIC GROUP

Automatable (A)

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.

<table>
<thead>
<tr>
<th>Metric Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No (N)</td>
<td>Attackers cannot reliably automate all steps of the kill chain for this vulnerability (reconnaissance, weaponization, delivery, and exploitation).</td>
</tr>
<tr>
<td></td>
<td>1. the vulnerable component is not searchable or enumerable,</td>
</tr>
<tr>
<td></td>
<td>2. weaponization requires human direction for each target,</td>
</tr>
<tr>
<td></td>
<td>3. delivery uses channels that network security configurations block</td>
</tr>
<tr>
<td></td>
<td>4. exploitation is not reliable, due to exploit-prevention techniques enabled by default</td>
</tr>
<tr>
<td>Yes (Y)</td>
<td>Attackers can reliably automate all steps of the kill chain (reconnaissance, weaponization, delivery, and exploitation).</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
Recovery (R)

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

<table>
<thead>
<tr>
<th>Metric Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic (A)</td>
<td>The Component/System recovers automatically after an attack.</td>
</tr>
<tr>
<td>User (U)</td>
<td>The Component/System requires manual intervention by the user to recover services, after an attack.</td>
</tr>
<tr>
<td>Irrecoverable (I)</td>
<td>The Component/System is irrecoverable by the user, after an attack.</td>
</tr>
</tbody>
</table>
Value Density (V)

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.

<table>
<thead>
<tr>
<th>Metric Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diffuse (D)</td>
<td>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.</td>
</tr>
<tr>
<td>Concentrated (C)</td>
<td>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.</td>
</tr>
</tbody>
</table>
WHAT’S NEW – SUPPLEMENTAL METRIC GROUP

Vulnerability Response Effort (RE)

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.

<table>
<thead>
<tr>
<th>Metric Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low (L)</td>
<td>The effort required to respond to a vulnerability is low / trivial.</td>
</tr>
<tr>
<td>Moderate (M)</td>
<td>The actions required to respond to a vulnerability require some effort on behalf of the consumer and could cause minimal service impact to implement.</td>
</tr>
<tr>
<td>High (H)</td>
<td>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.</td>
</tr>
</tbody>
</table>
WHAT’S NEW – SUPPLEMENTAL METRIC GROUP

Provider Urgency (U)

• 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:
  o 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.
WHAT'S NEW – SUPPLEMENTAL METRIC GROUP

Provider Urgency (U)

Metric Values:

The provider has assessed the impact of this vulnerability as having ...

<table>
<thead>
<tr>
<th>Metric Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red (R)</td>
<td>...the highest urgency</td>
</tr>
<tr>
<td>Amber (A)</td>
<td>...a moderate urgency</td>
</tr>
<tr>
<td>Green (G)</td>
<td>...a reduced urgency</td>
</tr>
<tr>
<td>Clear (C)</td>
<td>...low or no urgency (i.e.: Informational)</td>
</tr>
</tbody>
</table>
WHAT’S NEW – OT/SAFETY

• 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.
Provider Supplied Supplemental Metric “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:

<table>
<thead>
<tr>
<th>Metric Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Present (P):</td>
<td>Consequences of the vulnerability meet definition of IEC 61508 consequence categories of &quot;marginal,&quot; &quot;critical,&quot; or &quot;catastrophic.&quot;</td>
</tr>
<tr>
<td>Negligible (N):</td>
<td>Consequences of the vulnerability meet definition of IEC 61508 consequence category &quot;negligible.&quot;</td>
</tr>
<tr>
<td>Not Defined (X):</td>
<td>The value of this metric has not been defined for this vulnerability.</td>
</tr>
</tbody>
</table>

**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.
Customer 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.
WHAT’S NEW – OT/SAFETY

Customer Supplied Environmental Safety (Continued)

• Modified Integrity of Subsequent System: Safety (MSI:S)
  o 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)
  o 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).
AGENDA

• Introduction
• What’s New in CVSS v4?
• CVSS Best Practices
  o Technical Severity vs. Risk
  o Operationalization & Automation
• Wrap-it-up
TECHNICAL SEVERITY VS. RISK

• CVSS Base scores (CVSS-B) represent “Technical Severity”
  o Only takes into consideration the attributes of the vulnerability itself
  o 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...
  o Base Score
  o Threat associated with the vulnerability
  o 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.
OPERATIONALIZATION & AUTOMATION

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

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

• Introduction
• What’s New in CVSS v4?
• CVSS Best Practices
• Wrap-it-up
  o Important Links
  o Q & A
IMPORTANT LINKS

• CVSS SIG: https://first.org/cvss
  o CVSS v3.1 Specification: https://www.first.org/cvss/specification-document
  o CVSS v3.1 User Guide: https://www.first.org/cvss/user-guide
  o CVSS v3.1 Calculator: https://www.first.org/cvss/calculator

• CVSS Online Training Course: https://www.first.org/cvss/training

• CVSS v4.0 Work In Progress: https://www.first.org/cvss/v4-0
Q & A
THANK YOU!

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