Here Comes CVSS v4.0

Dave Dugal (Juniper Networks, USA)
Dale Rich (Black & Veatch, USA)
High-Level Accomplishments for CVSS v4.0

• Finer granularity in Base Metrics
  - Attack Requirements (AR) 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
Overarching Messages for CVSS v4.0

• Stress the difference between Technical Severity and Risk
• Include guidance on migration from CVSS v3.x to v4.0
• Highlight best current practices for correct usage of CVSS, including familiarity with documentation, and completed training
  • CVSS Scoring Certification?
• CVSS is not just the Base score (CVSS-BTE)

❖ CVSS v4.0 Public Preview targeting December 2022
  • Question, comments, and feedback welcome and encouraged
## CVSS v4.0: The Calculator


### CVSS v4.0 Calculator Mock-Up

<table>
<thead>
<tr>
<th>Base Score</th>
<th>Attack Vector (AV): Network (N)</th>
<th>Adjacent (A)</th>
<th>Local (L)</th>
<th>Physical (P)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack Complexity (AC): Low (L)</td>
<td>High (H)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Attack Requirements (AR): None (N)</td>
<td>Present (P)</td>
<td>High (H)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Privileges Required (PR): None (N)</td>
<td>Low (L)</td>
<td>High (H)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User Interaction (UI): None (N)</td>
<td>Passive (P)</td>
<td>Active (A)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality of Vulnerable System (Cv): None (N)</td>
<td>Low (L)</td>
<td>High (H)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Integrity of Vulnerable System (Iv): None (N)</td>
<td>Low (L)</td>
<td>High (H)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Availability of Vulnerable System (Av): None (N)</td>
<td>Low (L)</td>
<td>High (H)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality of Subsequent System (Cs): None (N)</td>
<td>Low (L)</td>
<td>High (H)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Integrity of Subsequent System (Is): None (N)</td>
<td>Low (L)</td>
<td>High (H)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Availability of Subsequent System (As): None (N)</td>
<td>Low (L)</td>
<td>High (H)</td>
<td></td>
</tr>
</tbody>
</table>

#### Threat Score

Exploit Maturity (E): Not Defined (X) | Unreported (U) | POC (P) | Attacked (A)

#### Environmental Score

Confidentiality Requirements (CR): Not Defined (X) | Low (L) | Medium (M) | High (H) | Physical (P) |

Integrity Requirements (IR): Not Defined (X) | Low (L) | Medium (M) | High (H) |              |

Availability Requirements (AR): Not Defined (X) | Low (L) | Medium (M) | High (H) |              |

Modified Attack Vector (MAV): Not Defined (X) | Network (N) | Adjacent (A) | Local (L) |              |

Modified Attack Complexity (MAC): Not Defined (X) | Low (L) | High (H) |              |

Modified Attack Requirements (MAR): Not Defined (X) | None (N) | Present (P) |              |

Modified Privileges Required (MPR): Not Defined (X) | None (N) | Low (L) | High (H) |              |

Modified User Interaction (MUI): Not Defined (X) | None (N) | Passive (P) | Active (A) |              |

Modified Confidentiality of Vulnerable System (MCv): Not Defined (X) | None (N) | Low (L) | High (H) |              |

Modified Integrity of Vulnerable System (MIv): Not Defined (X) | None (N) | Low (L) | High (H) |              |

Modified Availability of Vulnerable System (MAv): Not Defined (X) | None (N) | Low (L) | High (H) |              |

Modified Confidentiality of Subsequent System (MCs): Not Defined (X) | None (N) | Low (L) | High (H) | Safety (S) |

Modified Integrity of Subsequent System (MIs): Not Defined (X) | None (N) | Low (L) | High (H) | Safety (S) |

Modified Availability of Subsequent System (MAs): Not Defined (X) | None (N) | Low (L) | High (H) | Safety (S) |

#### Supplemenal Metrics

Automatable (AU): Not Defined (X) | No (N) | Yes (Y) |              |

Recovery (R): Not Defined (X) | Automatic (A) | User (U) |              |

Value Density (V): Not Defined (X) | Diffuse (D) | Concentrated (C) | Irrecoverable (I) |

Vulnerability Response Effort (VRE): Not Defined (X) | Low (L) | Moderate (M) | High (H) |              |

Provider Urgency (U): Not Defined (X) | White | Green | Amber | Red |