



CVSS Guidance Document

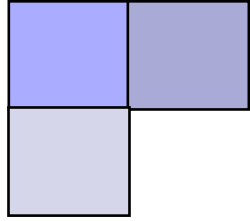
Chris Johnson
Peter Mell
Karen Scarfone
National Institute of Standards and Technology



Sponsored by
DHS National Cyber Security Division/US-CERT

National Vulnerability Database
a comprehensive cyber vulnerability resource

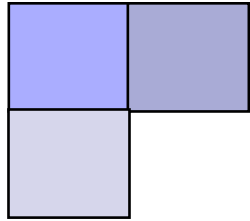
NIST
National Institute of
Standards and Technology



Intended Usage

- Official NIST publication in support of NVD operations
- Submitted to CVSS SIG as a basis for official SIG guidance

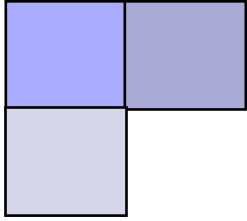




Goals of the CVSS Scoring Guidance Document:

- Identify current impediments to achieving the goals of the CVSS:
 - Consistency – repeatable scoring actions
 - Standardization – ability to normalize scores across disparate platforms
 - Transparency – ability to understand how the score was derived
 - Accuracy – correctly communicate vulnerability characteristics
- Analyze the scoring actions of the NVD Ops Team and the feedback received from the user community
- Identify the root causes for disparate scoring results
- Issue amplifying and clarifying guidance on the appropriate and consistent use of the CVSS
- Provide additional real-world scoring examples

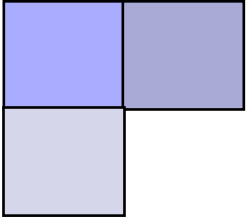




Sources

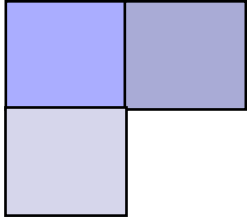
- National Vulnerability Database Operations Team
- Feedback received by NVD via email, web-based issue tracking, and outreach from:
 - Vulnerability Bulletin Providers
 - Security Product Vendors
 - Operating System, Application and Hardware Vendors
 - Vulnerability Researchers
 - Commercial Entities
 - Government Agencies
 - Educational Institutions
- Summer Undergraduate Research Fellowship researcher participation





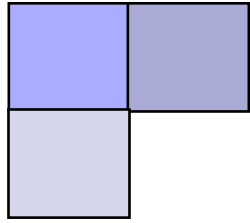
Areas of Interest





Natural Language Precision

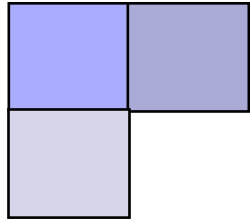
- Subjectivity, Imprecision or Uncertainty in vulnerability source data can lead to scoring discrepancies
 - Qualitative characterizations of vulnerabilities
 - “errors can *easily* be exploited...” (CVE-2007-0555)
 - Imprecision
 - “user having *appropriate* permissions” (CVE-2005-1984)
 - “under *some* configurations...” (CVE-2003-0352)
 - “Presumably, attackers could execute...” (CVE-2006-1368)
 - “possibly”
 - “theoretically”
 - Lexical and Semantic Uncertainty (weak phrases)
 - ““in certain circumstances...” (CVE-2006-3403)
 - “could allow an attacker...” (CVE-2007-0934)
- Need to promote greater precision in natural language vulnerability descriptions – strive for the same degree of specificity as found in a well-written requirements specification



Information Disclosure

- Complete and actionable data required to create CVSS scores is not always available.
- When this is the case, NVD analysts assign CVSS scores using a worst case approach (applies the highest rating)
- Results in loss of transparency and specificity

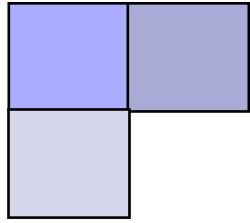




Multi-Vendor, Product, Version CVSS Scores

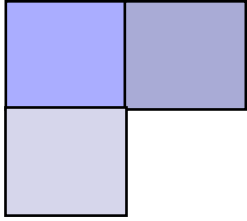
- CVSS scores applied to CVEs that span vendors, products or versions can lead to:
 - Diminished risk awareness
 - Decreased transparency (i.e., vector components become less meaningful)
 - Loss of specificity (i.e., how a particular product is affected)
 - Elevated base scores





Role of Trust Boundaries in Evaluating Impact Types

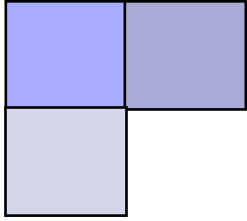
- Vulnerabilities that Bridge a Trust Boundary
 - Network Trust Zones
 - Application Trust Zones
- Vulnerabilities Within a Trust Zone



What is a system?

- Revisit the Definition of “System” in the context of CVSS
- What impact does the vulnerability have on the ability of the system to perform its primary business function?
 - Database Server
 - Web Server
 - DNS Server
 - Email Server
- Explore the user feedback that suggests that CVSS is operating system-centric

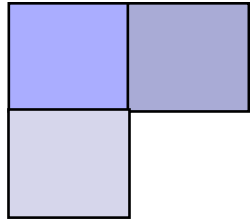




Contextual Dependencies

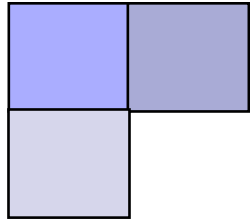
- Access Vector
 - Remote vs. Local can't readily be determined (e.g., an application that uses a faulty API or library)
- Privilege Level
 - User context under which the vulnerability is manifested (e.g. Root, Application, or User-Level)
 - CVSS General Scoring Tip #3, which recommends scoring be performed based on the most commonly used privilege
- Common Configurations
 - The basis for declaring something “common” is often disputed and rarely defensible due to lack of empirical data.
- Default Settings
 - Vendor Out-of-Box
 - U.S. Federal Desktop Core Configuration
 - U.S. DoD Settings





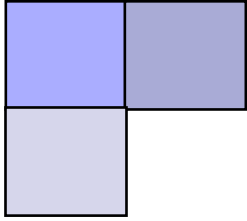
Preconditions

- Exploit requires presence of a specific:
 - Package
 - Role
 - Library
 - Module
- Vulnerability may manifest itself only in the presence of a particular product extension or configuration



Partial and Complete

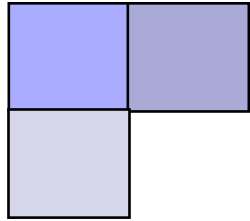
- Most often discussed in the context of scoring database issues
 - Partial rating does not provide sufficient granularity
(1%-99% of records/tables/files)
 - Partial+ (full compromise of the affected component)



Access Complexity

- Ability to Differentiate
 - Low is typically easy
 - Medium and High are viewed as less distinct
- Access Vector and Authentication (locally exploitable)
- XSS and issues surrounding direct vs. indirect impact

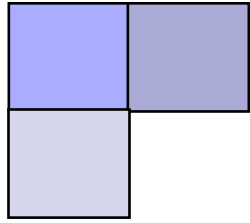




CVSS General

- Reinforce intended uses
- Identify use cases that are outside the scope of CVSS (e.g., blended threats)
- Address coupling of Integrity and Availability (i.e., when is integrity sufficiently degraded that it becomes an availability issue)

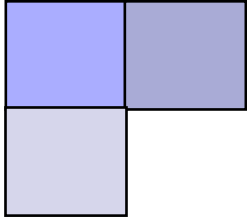




Proposed Schedule

- Research and Analysis (June-July)
- Internal Draft (July 25th)
- Submit to CVSS SIG for review (Late July)
- Publish Official Draft NIST Interagency Report (Mid-August)





Contact Information

Chris Johnson

(301)975-5981

christopher.johnson@nist.gov

Peter Mell

(301)975-5572

mell@nist.gov

Karen Scarfone

(301)975-8136

karen.scarfone@nist.gov

