- Sign in
- Contact
- Sitemap

- About FIRST
    - Mission Statement
    - History
    - Organization
        - Board of Directors
        - Secretariat
        - Member Teams
        - Liaisons
        - Committees
    - FIRST Policies
        - Bylaws
        - Whistleblower Protection Policy
        - Conflict of Interest Policy
        - Travel Policy
        - Document Record Retention and Destruction Policy
        - Uniform IPR Policy
        - General event registration refund policy
        - Identity & Logo Usage
    - Partners & Affiliates
        - Partnerships
        - Affiliates
    - Newsroom
        - What's New
        - Press Releases
        - In the News
        - FIRST Press Policy
- FIRST Members
    - Becoming a Member
        - Benefits
        - Membership Process
            - Full Member Form (App A)
            - Liaison Form (App B)

- Membership Fees
- Member Teams
- Liaison Members
- Members around the world
- Membership Application
    - Team Membership Application
    - Liaison Membership Application
    - Request for information

- Global Initiatives
    - Special Interest Groups (SIGs)
        - SIGs Framework
        - Common Vulnerability Scoring System (CVSS-SIG)
            - CVSS v3.0 Calculator
            - CVSS v3.0 Specification Document
            - CVSS v3.0 User Guide
            - CVSS v3.0 Examples
            - CVSS v3.0 Calculator Use & Design
            - CVSS v2 Archive
                - CVSS v2 Complete Documentation
                - CVSS v2 History
                - CVSS-SIG team
                - SIG Meetings
                - Frequently Asked Questions
                - CVSS Adopters
                - CVSS Links
            - CVSS v1 Archive
                - Introduction to CVSS
                - Frequently Asked Questions
                - Complete CVSS v1 Guide
                - CVSS Draft versions
                - CVSS links
            - CVSS-SIG participants
            - Scores and Calculators
            - Identity & logo usage
        - Ethics SIG
        - Information Exchange Policy SIG (IEP-SIG)
        - Internet Infrastructure Vendors (Vendor SIG)
            - Participating Vendors
            - Documents
        - Malware Analysis
        - Metrics SIG
        - Red Teaming
        - Traffic Light Protocol (TLP-SIG)
        - Vulnerability Coordination
            - Multi-Party Coordination and Disclosure
        - Vulnerability Reporting and Data eXchange SIG (VRDX-SIG)
            - Vulnerability Database Catalog
    - Best Practices Contest
    - Standards

        - Traffic Light Protocol (TLP)
        - Common Vulnerability Scoring System (CVSS-SIG)
        - Information Exchange Policy (IEP)
        - Passive DNS Exchange
    - Education Program
    - Fellowship Program
        - Application Form
    - Affiliates
    - Internet Governance
    - IR Database
    - Partnerships
- Events
    - Events Calendar
    - FIRST Events
        - Annual Conferences
            - Network Privacy Statement and Conference Monitoring
        - Technical Colloquia & Symposia
        - Training
- Meetings
    - Annual General Meeting
        - Board duties
    - CVSS SIG Meetings
- Security Library
    - Papers & Presentations
    - Best Practices Guide (BPGL)
    - Security Reference Index
    - Contribute to the Library
- Newsroom
    - What's New
    - Press Releases
    - In the News
    - FIRST Press Policy

Common Vulnerability Scoring System (CVSS-SIG)

- CVSS v3.0 Calculator
- CVSS v3.0 Specification Document
- CVSS v3.0 User Guide
- CVSS v3.0 Examples
- CVSS v3.0 Calculator Use & Design
- CVSS v2 Archive
- CVSS v1 Archive
- CVSS-SIG participants
- Scores and Calculators
- Identity & logo usage

Common Vulnerability Scoring System, V3

Development Update

June 10th, 2015

Third version aims to make the system more applicable to modern concerns

The Forum of Incident Response and Security Teams (FIRST) has today announced the availability of version 3 of the Common Vulnerability Scoring System (CVSS). The new system is the latest update of the universal open and standardized method for rating IT vulnerabilities and determining the urgency of response. Version 3 of CVSS has been under development for three years, with work initiated at the FIRST Conference in Malta in June 2012.

CVSS version 3 sets out to provide a robust and useful scoring system for IT vulnerabilities that is fit for the future. Its development has been overseen by the CVSS Special Interest Group (SIG) with input from representatives of a broad range of industry sectors, from banking and finance to technology and academia.

The updated version includes enhancements such as: the promotion of consistency in scoring, the replacement of Scoring Tips in order to more clearly guide end users of CVSS, and consideration of the system in order to make it more applicable to modern concerns. More information on the standard is available at https://www.first.org/cvss.

Seth Hanford, co-chair of the FIRST CVSSv3 working group said "We hope that CVSS version 3 is clear, consistent and repeatable, and able to support the work of those who seek to understand, describe, compare, or evaluate IT vulnerabilities via a common scoring system."

"Our aim has been to provide a system that is flexible enough to handle both the challenges that have emerged in vulnerability scoring in recent years, as well as those that we will see in the years to come."

December 12th, 2014

In this final preview of the Common Vulnerability Scoring System 3.0 (CVSS v3.0), the CVSS Special Interest Group (CVSS-SIG) has provided the following:

- Updated Metrics Descriptions and values for the CVSS v3.0 (cvss-v30-preview2-metricvectorstring-december-2014.pdf)
- Updated vector string notation to represent vulnerability's CVSS v3.0 score in an abbreviated format. (cvss-v30-preview2-metricvectorstring-december-2014.pdf)
- CVSS v3.0 Formula (cvss-v30-preview2-formula-december-2014.pdf) and online calculator (https://www.first.org/cvss/calculator/3.0)
- Examples Document (cvss-v30-preview2-examples-december-2014.pdf)

Although we delayed the release by a few weeks, the CVSS-SIG hopes that this final preview with complete formula and examples will provide the necessary detail and context to ensure a productive public assessment, and ultimately a robust standard that best meets the need of the security community at large.

As with preview release 1, it is our hope that teams will fully utilize access to this preview and begin to produce CVSS v3.0 scores alongside whatever other scoring system they are using today. When the completed CVSS v3.0 standard is approved, organizations that have stored scores produced via CVSS v3.0 previews and can use that data to offer official CVSS v3.0 scoring data.

That being said, some of the changes since preview 1 have material impact to the metric decisions made by the analysts and associated scoring outcomes. Therefore any vulnerabilities previously assessed with CVSSv3.0 Preview Release 1, will need to be updated to reflect changes made in Preview Release 2. Specifically:

- When to Calculate a CVSS v3.0 Score
- Availability Impact
- Attack Complexity

WHILE THE CVSS-SIG HOPES THAT MANY WILL TAKE ADVANTAGE OF THIS PREVIEW TO HELP THEMSELVES BECOME ACQUAINTED WITH THE STANDARD, WE ASK THAT NOONE USE THIS DOCUMENT TO GIVE OFFICIAL PUBLIC CVSS V3.0 METRICS OR VECTOR STRINGS TO VULNERABILITIES.

The CVSS-SIG does not want to discourage any public commentary regarding CVSS v3.0 preview 2, but we feel the community would be disadvantaged by anyone assigning CVSS v3.0 metrics in any official, public manner (such as in a product security advisory, as the results of a vulnerability scan, in a vulnerability database, etc.) before the final specification is released.

CVSS v3.0 Preview Release 2 Comments period will be open from publication of this document through February 28th 2015.

Please submit all comments to:
cvss-v3-comments@first.org

Max Heitman
Co-Chair, CVSS-SIG
max.heitman@citi.com

June, 2014

In this first preview of the Common Vulnerability Scoring System, version 3, the CVSS Special Interest Group (CVSS-SIG) has provided the descriptions and values for the CVSS v3 Metrics, as well as the vector string notation to represent a vulnerability¹s CVSS v3 score in an abbreviated format.

Upon release, it is our intention that recipients of this guide would begin to produce CVSS v3 scores alongside whatever other scores they are using today (CVSS v2, or other scores for vulnerabilities). When it is time to release the completed CVSS v3 formula, organizations that have stored scores produced via this CVSS v3 Preview will be able to use the stored scores to generate CVSS v3 numeric scores.

The CVSS-SIG hopes that this preview will give additional lead time to incident response teams, analysts, and those doing vulnerability rating and classification with CVSS or similar systems. Because rating and classification typically is the more time-intensive activity, we encourage teams to start early and produce scores for storage as soon as possible. This will give incident responders and analysts additional time to practice CVSS v3 scoring, and to help ease their transition into CVSS v3.

While the CVSS-SIG hopes that many will take advantage of this preview to help themselves become acquainted with the standard, we ask that noone use this document to give official public CVSS v3 metrics or vector strings to vulnerabilities.

The CVSS-SIG does not want to discourage any public commentary regarding CVSS v3 preview metrics or vector strings, but we feel the community would be disadvantaged by anyone assigning CVSS v3 metrics in any official, public manner (such as in a product security advisory, as the results of a vulnerability scan, in a vulnerability database, etc.) before the final specification is released.

Seth Hanford
Chair, CVSS-SIG
seth@first.org
@SethHanford

Please submit general comments on this Preview to:
cvss-v3-comments@first.org

March 15th, 2013

With the release of an open letter to FIRST regarding CVSS v2, I wanted to take some time to update the security community on some of the work that has been going into the development efforts toward CVSS v3. For reference, that OSVDB letter was posted here:
http://blog.osvdb.org/2013/02/27/cvssv2-shortcomings-faults-and-failures-formulation

More details about the background including the Call for Papers and SIG selection process can be found online:
https://www.first.org/cvss/v3/development

First of all, on behalf of the SIG I'd like to express my thanks to Carsten Eiram and Brian Martin for posting their thoughts on some of the challenges with CVSS v2. Back in April 2012 the CVSS-SIG opened its Call for Subjects to solicit input from the community regarding proposed improvements to CVSS. Since June 2012, the SIG has been working on classifying and categorizing those subjects, developing a plan of attack, and working through how to implement solutions to those subjects which the SIG believes are in scope for CVSS and would represent a significant improvement to the standard.

As I read the OSVDB letter, I was struck by how similar the complaints and suggestions found in it lined up with the proposed subjects we received back in early 2012, though neither Mr. Eiram or Mr. Martin, nor any representatives from Open Security Foundation, Risk Based Security, or OSVDB submitted subjects during the Call. I believe that this provides confirmation that we have succeeded in capturing the community's requirements for improving CVSS. I'll highlight here some of the broad efforts of the SIG, which address these and other points which the community has told us need improvement in CVSS v3.

The CVSS v3 development process is ongoing; our draft is due by the end of this year, with a completed and approved specification expected in Summer 2014 (most likely to coincide with the FIRST Annual Conference). That being said, some of what I'm sharing here is work that has been completed, proposed, and voted for approval by the SIG; other work is in progress and should not be considered fully formed. Please take this letter as a view into the process, and an encouragement for more feedback.

Seth Hanford
Chair, CVSS-SIG
seth@first.org

The "Scope" Problem

By far, the most frequently and passionately communicated problem that we have heard from the community is that the v2 concept of impacts being scoped to the host operating system (Section 3.1.1, Scoring Tip #2). This problem also manifests itself in other ways, but has also become more prevalently encountered as virtualization and sandboxing moved into the mainstream since the 2007 release of CVSS v2. It has resulted in community-led solutions like Oracle's inclusion of "+" on any Partial scores which could (from a non-host-centric perspective dictated by CVSS v2) be considered a "Complete" compromise (from an application or component-centric perspective). This problem has also meant that extra-host impacts like those encountered by network devices are very poorly represented.

This is not an easy problem to solve in a repeatable and simple manner, which promotes consistency in scoring (one of CVSS' fundamental goals). The concepts related to scoping make sense intuitively to many people, but some subtle challenges have given us some very real problems, not the least of which is documentation which would clearly solve the issue without opening the door to wildly inconsistent application of the scoring system. There is a proposal in place which would address scope in a fairly comprehensive manner, and which could directly or indirectly solve the "Cyberspace Five-O Problem", "Plus-sized Scoring Problem" (p. 3), as well as some issues expressed in "Sandbox Escape Reality Deviation" (p. 9).

CVSS v2 was a major improvement over v1, in no small part because one of the most voiced concerns (that single "Complete" impacts could score lower than multiple "Partial" impacts) was addressed. I don't believe that solving the "scope" problem is any less important for CVSS v3. It may not be possible to address this cleanly, and it may be a fundamental problem for CVSS for some time, but our hope is that it becomes a major improvement that drives many users to adopt CVSS v3 as a significant improvement over v2.

The "Scoring Tips" and Other Inconsistencies

As mentioned previously, consistency is a core requirement for CVSS. It's one of the meanings of "Common" for the "Common Vulnerability Scoring System". During the documentation process for v2, "Scoring Tips" were included with the hope that they would guide users of the system to overcome common headaches or questions that were encountered by the SIG team. Unfortunately, even the name "Tips" suggests that they might be optional.

A "Scoring Philosophy" or similar guidance, in place of Scoring Tips, should help to more clearly guide end users of CVSS. Right now, many of the letter's issues center around differing approaches used by vendors and vulnerability intelligence services / vulnerability databases that provide scores. This will never be entirely eliminated, however there are areas where CVSS as a specification can provide clearer guidance, and we intend to do so.

Further, there are other subtle ambiguities that were uncovered during a review of metric frequencies. We have taken the stance that for v3, we will first avoid subjective choices whenever possible, and if that is not practical then we will strive for other means to limit their impact to the resulting score, including some ideas we have about weighting subjective choices for metrics more closely than we weight metric choices that have unambiguous or objective choices. For example, when considering User Interaction (a new metric in v3 with options for "None", "Simple", and "Complex") we might have a large weight difference between None and Simple, while the weights between Simple and Complex might be weighted more closely, due to an inability to clearly and objectively delineate the differences between Simple and Complex User Interaction.

Complexity and Other Multi-use Metrics

Access Complexity is a very overloaded and subjective metric in CVSS v2. When it's applied, it's impossible to tell if it's being used for user interaction from social engineering, from a race condition, uncommon configuration, attacker starting privileges, or anything else. As more or less a catch-all for CVSS v2, it has gotten a lot of negative feedback.

This certainly does not help CVSS v2 with regard to repeatable and clear scoring. As a result, the CVSS-SIG has taken a few steps to improve the consistency of Access Complexity, one of which I've already mentioned: User Interaction now stands on its own. Given the prevalence of code execution vulnerabilities that require the user to visit a malicious web site or open a malformed document since CVSS v2, we believe that there is a significant justification for specifically calling these vulnerabilities out in individual metrics. This also promotes clarity, as in the "Access Vector: Context Dependent" cases suggested in the OSVDB letter.

The SIG will also be looking at Access Vector to see if we can make better distinction between Physical and Local attackers, as those are both lumped under "Local" in v2.

Authentication vs. Privilege

Another item that rose to our attention with statistical analysis of the CVSS v2 data was that Authentication: Multiple was rarely, if ever, used. So in v3, we are looking at measuring the privileges required by the attacker, instead of whether or not they are authenticated. This will answer a number of issues with CVSS v2, including the some of the "Context Dependent" issues, "Authentication Bifurcation" (it is specifically the attacker's privileges; the user's privilege gained in a User Interaction flaw will be reflected by the Impacts), and will assist with "Locality Certainty".

Chaining vulnerabilities

Finally, there are some areas where CVSS v3 hopes to make itself more applicable to modern concerns. It's clear that CVSS should always be scoped to individual vulnerabilities. If not, there's room for inflation of severity and fear−mongering as many vulnerabilities could be combined to "make mountains out of mole hills".

But at the same time, vulnerabilities do not always exist (or get exploited) in isolation. Therefore, we hope to provide guidance on how to provide (and explicitly specify) CVSS scores for multiple related vulnerabilities. That is to say, when one or more vulnerabilities make conditions or resources available to an attacker that are required in order to exploit follow-on vulnerabilities that are also present, then it makes sense to derive a score for that chain of vulnerabilities.

In some cases, chains will expose a series of low-impact vulnerabilities that result in a final, higher impact. In others, chains will describe how rollbacks, downgrades, or regressions in software can be exploited to reintroduce prior vulnerabilities from earlier, more vulnerable versions to newer software.

In all cases, CVSS will require that each vulnerability be given its own, independent score. Then, the chain of vulnerabilities can be described and given a combined score for the chain itself. Chains might be described specifically (such as one CVE chained with one or more other CVEs) or generically (such as one or more vulnerability classes or CWEs being chained in order to exploit a specific CVE). But in the end, we believe that we could add value through CVSS to common scenarios without sacrificing the integrity of a scoring system that specifically addresses distinct vulnerabilities independent of each other.

Conclusion

The CVSS−SIG has been hard at work over the last several months, and there is quite a bit of work left to do before our target release date in June 2014. We haven't answered exhaustively all of the points raised in the OSVDB letter, but instead continue to take their points and examples alongside the other submissions to the Call for Subjects into consideration as we move on toward the goal of an improved CVSS v3 revision.

In many cases, the problems they raised can be dealt with through better documentation that drives consistency of scoring execution; in other cases, their proposals or something similar should accomplish a more granular, specific, actionable or complete scoring system. Overall, the SIG hopes that CVSS v3 will be clear, consistent, and repeatable, as well as flexible enough to handle not only the challenges that have arisen in vulnerability scoring in the last several years, but for a few years to come.

Please consider subscribing to cvss−sig@first.org, or reaching out to me directly with input. I and other members of the SIG will also be looking for opportunities to present publicly in the coming months as the drafts progress, at FIRST venues and elsewhere as we are able. Thank you again for your interest and investment in using and improving CVSS, and ultimately in working to make security more measurable and mature.

Announcing the CVSS Special Interest Group

for CVSS v3 Development

On May 14, 2012, the FIRST Board approved the roster for the CVSS Special Interest Group (SIG) team that will oversee the development of CVSS v3. Based upon applications received in response to the Call for Participants, the FIRST Board has approved a team designed to address open concerns with CVSS v2 and ensure that CVSS v3 provides the necessary enhancements for achieving the mission of the scoring standard: To support the work of those who seek to understand, describe, compare, or evaluate information technology vulnerabilities via a common scoring system.

From the pool of applicants, the FIRST Board selected 19 individuals from 8 of the 10 proposed constituencies. Membership in the SIG received significant interest and while the Board was unable to accommodate all applicants with a voting membership on the SIG, anyone interested in CVSS will be able to participate during the open discussion regarding the standard. As part of the evaluated requirements, each voting member will be required to work with other organizations in the same constituency to provide input to the standard.

Participants were selected based on:

- We chose to seek a balance between new and veteran members for each of the constituencies;
- Participants were selected in order to allow constituencies to be of roughly equal size, and prevent one constituency from dominating the discussion during voting. However, anyone is welcome to participate in the CVSS discussions and SIG meetings. Only voting is restricted to the selected representative individuals.
- Applicants were requested to provide a proposal on how they will interface with non-voting members in the same constituency to ensure their feedback is sufficiently taken into account. The strength of this proposal was considered.

Above all, the FIRST Board would like to thank everyone who took time to apply for the SIG and congratulate those who were selected.

Work will officially begin on version 3 during the 2012 FIRST Annual Conference, June 17. Until then, those interested in participating in shaping the direction for CVSS can answer the Call for Subjects (https://www.first.org/newsroom/releases/20120411). Those who applied for SIG membership and were not selected as SIG members, or those who missed the application deadline for the Call for Participants, are still welcome to participate in the standard and are encouraged to notify seth@first.org for further instructions.

Banking / Finance:

- Max Heitman, Citi (Co-Chair)
- Michael Chernin, Depository Trust & Clearing Corporation
- Seth Hanford, TIAA-CREF

Government:

- David Waltermire, NIST
- Martijn de Hamer, NCSC-NL

- Masato Terada, Information-Technology Promotion Agency Japan

Academic:

- Sasha Romanosky, PhD, Carnegie-Mellon University
- Karen Scarfone, Scarfone Cybersecurity

Manufacturing / Retail:

- Bruce Monroe, Intel

Technology:

- Arjuna Shunn, Microsoft
- Kierron Shorrock, VMware
- Bruce Lowenthal, Oracle

Telecommunications:

- Dave Dugal, Juniper
- Seth Hanford, TIAA-CREF (Chair)

CIRTs & Security Research:

- Scott Moore, IBM
- Art Manion, CERT
- Arnold Yoon, Dell

Energy:

- Jeffrey Heller, Sandia National Laboratories

About CVSS

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base group represents the intrinsic qualities of a vulnerability, the Temporal group reflects the characteristics of a vulnerability that change over time, and the Environmental group represents the characteristics of a vulnerability that are unique to a user's environment. The Base metrics produce a score ranging from 0.0 to 10.0, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. This document provides a collection of examples of vulnerabilities scored using CVSS v3.0.

About FIRST and CVSS-SIG

CVSS is owned and managed by FIRST.Org, Inc. (FIRST), a US-based non-profit organization, whose mission is to help computer security incident response teams across the world. FIRST reserves the right to update CVSS and this document periodically at its sole discretion. While FIRST owns all right and interest in CVSS, it licenses it to the public freely for use, subject to the conditions below. Membership in FIRST is not required to use or implement CVSS. FIRST does, however, require that any individual or entity using CVSS give proper attribution, where applicable, that CVSS is owned by FIRST and used by permission. Further, FIRST requires as a condition of use that any individual or entity which publishes scores conforms to the guidelines described in this document and provides both the score and the scoring vector so others can understand how the score was derived.

Chairs

Seth Hanford and Max Heitman

Available in PDF Format

- CVSS v3.0 Preview 2 - Metrics/Vector String
- CVSS v3.0 Preview 2 - Formula
- CVSS v3.0 Preview 2 - Examples
- CVSS v3 Preview 1 - Metrics
- CVSS v3 Bangkok Update (1.2M)
- CVSS v3 Development Update (47K)
- March 2013 Update (60K)
- CVSS v3 announcement (52K)
- FIRST CVSS IPR Policy (84K)