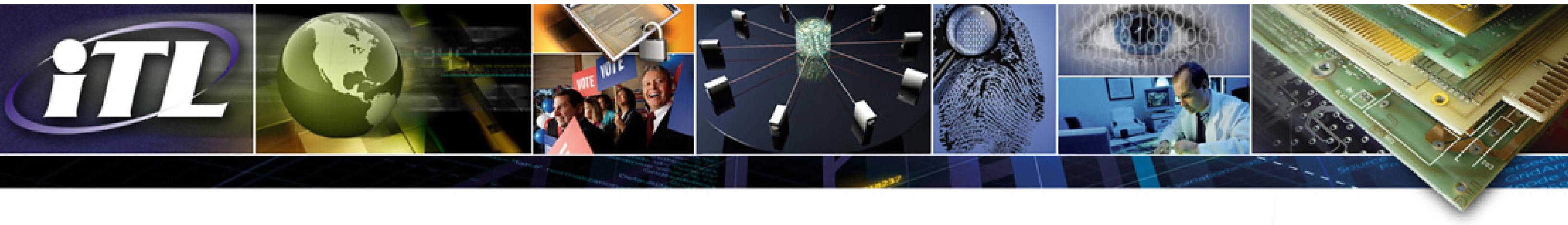


ITL BULLETIN FOR JULY 2014

RELEASE OF NIST INTERAGENCY REPORT 7946, CVSS IMPLEMENTATION GUIDANCE

Harold Booth, Joshua Franklin, Larry Feldman, and Greg Witte, Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Background

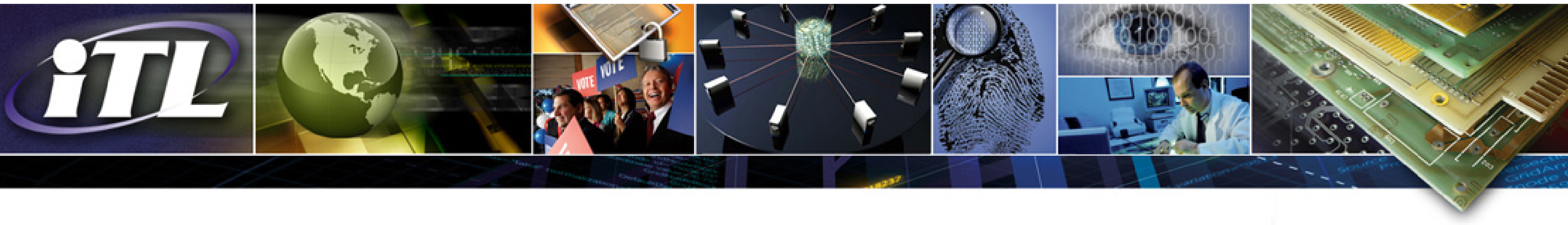
The Common Vulnerability Scoring System (CVSS) is an open standard designed to convey severity and risk of information system vulnerabilities. CVSS was commissioned by the National Infrastructure Advisory Council (NIAC) in support of the global Vulnerability Disclosure Framework. It is currently maintained by the Forum of Incident Response and Security Teams (FIRST).

The metrics and equations in CVSS were designed to be reasonably complete, accurate, and easy to use. They reflect the cumulative experience of the CVSS Special Interest Group, CVSS-SIG, as well as extensive testing of real-world vulnerabilities in end-user environments. The CVSS is an important tool that supports the National Vulnerability Database (NVD), a product of ITL's Computer Security Division and sponsored by the Department of Homeland Security's National Cyber Security Division.

Introduction to NISTIR 7946

In April 2014, NIST released Interagency Report (NISTIR) 7946 to provide transparency into NIST's processes, primarily describing how analysts at the NVD calculate base scores using CVSS Version 2.0 (CVSS v2.0). This transparency and clarity are helpful for organizations that rely on CVSS results, and they inform the vendor community about NIST scoring processes. The report provides detailed templates that describe the key words that help NVD analysts determine the potential severity of a given vulnerability, and describes the specific scoring practices used each day.

NISTIR 7946 assists individuals and organizations who wish to score vulnerabilities via the CVSS v2.0. The CVSS v2.0 defines a vulnerability as a bug, flaw, weakness, or exposure of an application, system device, or service that could lead to a failure of confidentiality, integrity, or availability. The document is intended to serve as a supplement to the CVSS v2.0 specification, providing additional guidance for difficult and/or unique scoring situations. The guidance in the document is the result of applying the CVSS v2.0 specification to over 50,000 vulnerabilities scored by analysts at the NVD. In particular, the NISTIR provides a list of more than 25 useful example vulnerabilities scored via the CVSS to assist vulnerability analysts. The scores are based on information provided by the NVD and include the Common Vulnerabilities and Exposures Identifier (CVE ID), Common Weakness Enumeration Identifier (CWE ID), CVSS base score, CVSS vector, a description of the vulnerability, and a justification for each CVSS base score.



The CVSS v2.0 specification describes CVSS v2.0 as an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS v2.0 consists of three groups: Base, Temporal, and Environmental. Each group produces a numeric score ranging from 0 to 10 and a Vector, a compressed textual representation that reflects the values used to derive the score. The Base group represents the intrinsic qualities of a vulnerability. The Temporal group reflects the characteristics of a vulnerability that change over time. The Environmental group represents the characteristics of a vulnerability that are unique to any user's environment. While the report does not provide guidance for assessing the temporal and environmental metric groups, end-user organizations should obtain or assign values for all metric groups to fully determine the consequence of a vulnerability. CVSS v2.0 enables IT managers, vulnerability bulletin providers, security vendors, application vendors, and researchers to all benefit by adopting this common language of scoring IT vulnerabilities.

CVSS v2.0 Limitations and CVSS v3

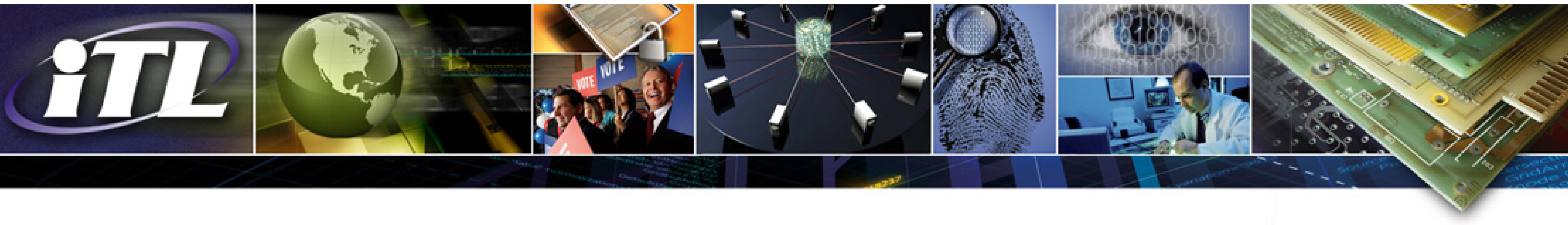
NISTIR 7946 highlights some limitations of version 2.0. The recent Heartbleed Bug (CVE-2014-0160) can provide a helpful example: according to CVSS v2.0, a weakness in a single application on a system would typically be considered "partial" impact. Such a loss, however, may underestimate the potential impact of a vulnerability when that single application is a significant element of the system's purpose (such as a web service application on a web server device). The result is a CVSS v2.0 Base Score (in this case, 5.0) that does not accurately reflect the severity of the vulnerability.

One challenge of CVSS v2.0 is the concept of impacts being scoped to the target host only. The specification includes scoring tip #2 that directs the reader to "consider the direct impact to the target host only." Members of the security community have pointed to the need for more levels to describe the potential impact of a vulnerability, beyond the current "None," "Partial," and "Complete." The need for more levels has resulted in solutions like Oracle's use of a proprietary impact type known as "Partial-Plus" ("Partial+") to address circumstances between truly partial compromise and complete. In addition, impacts beyond the host, like those encountered by network devices, are poorly represented. These challenges also make it difficult to produce a score for many client/server vulnerabilities such as those that include "DNS Cache attacks" (e.g., "Kaminsky bug," CVE-2008-1447) and "cross-site scripting" attacks that accurately conveys the severity of the vulnerability.

FIRST has announced that CVSS version 3 (CVSS v3) is under development. CVSS v3 is expected to address the challenges above and provide the model to more accurately score the potential impact of such vulnerabilities.

Ongoing Use of CVSS

CVSS v2.0 scores, such as those provided by vendors or the NVD, are based upon general characteristics of the vulnerability that does not consider local environment. Reliance on the CVSS base metrics without accounting for temporal aspects or environmental specific circumstances of a vulnerability may lead to organizations improperly measuring the severity of a vulnerability for their situation. While CVSS v2.0 provides some ability to consider environmental impact metrics, those metrics do not account for all environmental mitigating factors. The context of an environment could increase or decrease the ability



to exploit a particular vulnerability and affect the vulnerability severity. End-user organizations may wish to prioritize vulnerability response based on timely threat information, measured by the Exploitability vector in the temporal metrics.

Vulnerability assessment via CVSS can assist in conducting risk assessments, but CVSS scores should not be the sole factor when determining risk. The CVSS scores do not provide an aggregate score of a complete information system, and one should not sum up the scores to determine a final score for a system. Additionally, the CVSS score represents the impact of an individual vulnerability residing within an information system, and does not account for vulnerability chaining. Vulnerability chaining is the situation where multiple vulnerabilities are used together to perform an attack on a system. While CVSS is helpful to consider the severity of individual vulnerabilities, such vulnerabilities do not always exist (or get exploited) in isolation. In some cases, an exploitation of one or more vulnerabilities provides an attacker with a way to exploit follow-on vulnerabilities that are also present. These cases point out the need to derive a score for the chain of vulnerabilities. This is a combined score for the chain itself.

Conclusion

ITL has published Interagency Report 7946 to assist the vulnerability management community to better understand scoring methods and to advance development of the CVSS specification. CVSS users are encouraged to remain aware of ongoing efforts to improve the specification and contribute to that development.

Additional Resources

Joshua Franklin, Charles Wergin, Harold Booth, NISTIR 7946, *CVSS Implementation Guidance* - Direct link

Peter Mell, Karen Scarfone and Sasha Romanosky, *A Complete Guide to the Common Vulnerability Scoring System Version 2.0 (CVSS)*, Forum of Incident Response and Security Team (FIRST), June 2007.

Common Vulnerability Scoring System Version 3 Development Update

See ITL's information security programs, projects and research. All security publications (standards, special publications, guidelines, interagency reports and related papers are available from our Computer Security Resource Center.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.