Proposal to recast CVSS base score equation to improve correlation between scores and exploits

Ben Church – 10006197

Mohammed Alghamdi

**Introduction**

Software vulnerabilities are discovered and reported at rates which exceed security and reliability teams’ capacities to address them. To make better use of limited time and resources, vulnerabilities must be prioritized based on the risk they pose to the affected companies. The Common Vulnerability Scoring System (CVSS) was developed to meet this need. The CVSS provides several scores based on metrics pertaining to the vulnerability in question, the base score, temporal score, and environmental scores. The base score conveys the risk inherent in the vulnerability by using metrics which describe both the likelihood of exploitation, and the severity of the consequences of an exploitation.

**Problem Description**

Vulnerabilities’ CVSS base scores are often poorly correlated with instances of exploitation of these vulnerabilities. Allodi and Massacci [1], investigated the effectiveness of the CVSS for predicting real exploitation in a retroactive study. They examined entries in the National Vulnerability Database (NVD - <https://nvd.nist.gov/>) which reports a large number of vulnerabilities with their CVSS base score. The frequencies of these vulnerabilities’ appearances in several databases reporting exploits in the wild by vulnerability allowed them to correlate CVSS scores with exploitation. They found that prioritizing vulnerabilities based on their CVSS base scores was equivalent to fixing vulnerabilities in a random order in terms of the amount of exploits which would have been prevented.

Therefore the CVSS base score does not fulfill its intended function of conveying the risk inherent in the vulnerabilities. Some companies respond to the vulnerability prioritization problem with scoring systems of their own. For example, Mozilla1, and Google2 have vulnerability reward programs (VRPs). These programs offer cash rewards for reports of vulnerabilities in their software, providing economic incentives against selling the vulnerabilities to the black market. Younis *et al*. [2] remarks that Chrome vulnerability reports provided with proof of exploitation are more likely to result in a financial reward. Different organizations resorting to their own vulnerability ranking systems rather than using the CVSS, a scoring system purpose-designed for standardization of vulnerability comparison, reflects the power of economic selection pressure over academic inclination. However the issue of standardization remains, if one hopes create opportunities for cooperation and specialization among corporations facing an increasing number of vulnerabilities to address, or to develop tools as a third party for others to use.

The form of the CVSS base score equation is meant to reflect both the risk of a vulnerability being exploited, and the severity of the consequences if exploitation occurs. Arguably, with the exception of the Access Complexity metric, the metrics used to compute the base score are quantitative and unambiguous. For example, there is should be no ambiguity in whether a vulnerability requires zero, a single, or multiple instances of user authentication to exploit. The impact metrics, pertaining to system confidentiality, integrity, and availability, reflect whether none, some but not all, or all of each of these can be compromised on a system with the vulnerability. This reduces variability due to human factors, towards consistent standardization. The base score equation however, contains numerical values the metric variables can take on depending on their cases, and a number of scalar factors. For example, the Impact and Exploitability sub-scores are multiplied by 0.6 and 0.4, respectively, in computation of the final base-score. The variable and scalar values are apparently arbitrarily assigned to reflect the relative importances of the various metrics and sub-scores in the determination of the overall base score. Human subjectivity may enter the scoring system through the particular choices for these values.

**Proposed Work**

A better correlation between CVSS base score values and exploitation probability in the wild might be achieved by varying a subset of m of the n scalar parameters in the equation as an m-dimensional optimization problem. The variable to be optimized is some correlation coefficient between the CVSS base score and vulnerability exploitation probability. Possible choices for these parameters are highlighted with yellow in the base score equation, in the appendix. There are n = 26 in v2.10 of the CVSS base score equation. These may be varied largely independently, subject to natural constraints. For example, when an Impact metric indicates complete failure, the variable should take a larger value than when the failure is partial or non-existent. With each iteration of the base score equation’s parameters, the base scores for all vulnerabilities under consideration can be computed immediately.

Before the recast base scores can be correlated with exploit probability, this probability must be quantified. Bozorgi *et al.* [3] classified vulnerabilities from the Open-Source Vulnerability Database (OSVDB - <https://blog.osvdb.org/>) based on whether the vulnerability report was classified as having available or rumored/private exploits indicating positive exploit occurrences, or classified as unavailable or unknown exploits indicating negative exploit occurrences. Vulnerabilities with unclassified exploit statuses were not considered.

**References**

[1] Allodi L, and Massacci F. “Comparing Vulnerability Severity and Exploits Using Case-Control Studies” ACM Transactions on Information and System Security. 2014; 17(1):1-20.

[2] Younis AA, Malaiya YK, and Ray I. “Evaluating CVSS Base Score Using Vulnerability Rewards Programs” International Federation for Information Processing. 2016, 471:62-75.

[3] Bozorgi M. Lawrence KS, Savage S, and Voelker GM. 2010 “Beyond Heuristics: Learning to Classify Vulnerabilities and Predict Exploits” Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining. 2010; 105-114.

**Appendix**

The base equation is the foundation of CVSS scoring. The base equation (v2.10) is:

BaseScore = round\_to\_1\_decimal(((0.6\*Impact)+(0.4\*Exploitability)–1.5)\*f(Impact))

Impact = 10.41\*(1-(1-ConfImpact)\*(1-IntegImpact)\*(1-AvailImpact))

Exploitability = 20\* AccessVector\*AccessComplexity\*Authentication

f(impact)= 0 if Impact=0, 1.176 otherwise

AccessVector = case AccessVector of

requires local access: 0.395

adjacent network accessible: 0.646

network accessible: 1.0

AccessComplexity = case AccessComplexity of

high: 0.35

medium: 0.61

low: 0.71

Authentication = case Authentication of

requires multiple instances of authentication: 0.45

requires single instance of authentication: 0.56

requires no authentication: 0.704

ConfImpact = case ConfidentialityImpact of

none: 0.0

partial: 0.275

complete: 0.660

IntegImpact = case IntegrityImpact of

none: 0.0

partial: 0.275

complete: 0.660

AvailImpact = case AvailabilityImpact of

none: 0.0

partial: 0.275

complete: 0.660