Poster: On the Disconnect between CVSS Scores and Vulnerability Bounties

Nuthan Munaiah
nm6061@rit.edu

Andrew Meneely
axmvse@rit.edu

Department of Software Engineering
Rochester Institute of Technology, Rochester, New York, USA

ABSTRACT

The Common Vulnerability Scoring System (CVSS) has been a standard for vulnerability severity assessment. The U.S. National Vulnerability Database (NVD) mandates CVSS base scoring of all vulnerabilities that it curates. The CVSS metrics, however, go unused when software vendors are looking to reward ethical hackers with monetary benefits ("bounties") for responsibly disclosing vulnerabilities. In this poster, we present the findings from an empirical evaluation of the relationship (or lack thereof) between the two conceptually-related metrics: CVSS score and vulnerability bounty.

We collected the CVSS scores and bounties for 851 vulnerabilities across 28 products. A simple Spearman's rank correlation analysis revealed a weak correlation ($\rho = 0.2799$) between CVSS scores and vulnerability bounties. Hypothesizing that the weak correlation may be due to differences in concerns, we qualitatively compared the severity assessment criteria in CVSS to those in bounty determination guidelines. We found that 22 of the 34 bounty determination criteria are not explicitly mentioned in the CVSS specification. The results indicate that CVSS metrics lack the specificity of bounty determination guidelines, leading to a tenuous relationship between CVSS score and bounty.

CCS Concepts

•Security and privacy → Software security engineering; •Software and its engineering → Maintaining software;

Keywords

vulnerability, severity, bounty

1. INTRODUCTION

In a modern digital world, we must engineer software to be secure. A software vulnerability represents a potentially catastrophic engineering failure that can have widespread consequences for customers, patients, and citizens. However, not all vulnerabilities are the same; some are more severe than others. Software vendors need to prioritize vulnerabilities for purposes of threat dissemination, patching, and release management. Preferably, the prioritization method should be systematic, repeatable, and capture the nuances of the vulnerabilities' impact on a system and its users.

The Common Vulnerability Scoring System (CVSS) is the de facto standard for measuring vulnerability severity. Industry standards, such as those used by the Payment Card Industry (PCI) [5], rely on CVSS scores when auditing affiliated products. PCI considers a product to be non-compliant if a vulnerability with CVSS base score higher than 4.0 is found.

The CVSS "base" metrics are six multiple-choice questions that get averaged into a number from zero to 10. Critics of the CVSS argue that its weighting scheme lacks a transparent origin and that the questions are broad and subjective (e.g. "Is the access complexity low, medium, or high?").

Vulnerabilities are not a mere inconvenience to users, they are a business model for the unscrupulous. Vulnerabilities have monetary value [2]; the higher the damage that an attacker could inflict by exploiting the vulnerability, the higher is its value [1]. In an attempt to contain the threat of vulnerabilities being traded on the black market, software vendors and security companies have established bug bounty programs in which researchers are paid a *bounty* for reporting vulnerabilities.

If the bounty awarded is based on vulnerability severity, one would hope that vulnerability bounty and CVSS empirically align to some degree. We conducted an empirical study to investigate the relationship between CVSS scores and vulnerability bounties and found them to be weakly correlated ($\rho = 0.2799$). We then conducted a qualitative study to explain the weak correlation and found that 22 of the 34 bounty determination criteria are not explicitly mentioned in the CVSS specification.

In this poster, we present the findings from the study, which is based on our prior work [4] but with an extended data set. The data set was composed from CVSS score and vulnerability bounty data collected for 851 vulnerabilities across 28 products and is available on GitHub Gist [3].

2. REFERENCES

[1] A. Algarni and Y. Malaiya. Software Vulnerability Markets: Discoverers and Buyers. *International Journal on Computer, Information, Systems and Control Engineering*, 8(3):449–459, 2014.

[2] S. Frei and F. Artes. International Vulnerability Purchase Program. Technical report, NSS Labs, 2013.

[3] N. Munaiah and A. Meneely. Vulnerability Bounty Data Set. `https://gist.github.com/nuthanmunaiah/fe6a7e8e3cc4dbae84dc`. Accessed: 2016-12-14.

[4] N. Munaiah and A. Meneely. Vulnerability Severity Scoring and Bounties: Why the Disconnect? In *Proc. 2nd Int. Workshop on Software Analytics*, SWAN 2016, pages 8–14, New York, NY, USA, 2016. ACM.

[5] PCI SSC. Requirements and Security Assessment Procedures v3.1. pages 1–115, Apr 2015.