# On the Disconnect between CVSS Scores and Vulnerability Bounties

Nuthan Munaiah and Andrew Meneely
Rochester Institute of Technology, Rochester, NY

## Introduction

Security vulnerabilities in software systems are an inevitable reality

Software vendors need to effectively communicate the impact of vulnerabilities

Severity of a vulnerability is one way of quantifying its impact

Common Vulnerabilities Scoring System (CVSS) is the most commonly used vulnerability severity assessment method

In recent years, software vendors have been rewarding security researchers for responsibly disclosing vulnerabilities

One would assume the reward (called bounty) to be commensurate with severity, but is it?

## Common Vulnerability Scoring System (CVSS)

CVSS specifies base, environmental, and temporal metrics

National Vulnerability Database (NVD) requires base metrics

Access Vector  Authentication
Access Complexity

Availability Impact  Integrity Impact
Confidentiality Impact

Exploitability Metrics (Exploitability Subscore)

Impact Metrics (Impact Subscore)

Base Metrics (Base Score)

Six base metrics correspond to six multiple choice questions:

Where must the attacker be?
- Local
- Adjacent Network
- Network

What level of authentication is needed?
- None
- Single
- Multiple

How complex is it to access?
- Low
- Medium
- High

What is the potential for availability compromise?
- None
- Partial
- Complete

What is the potential for integrity compromise?
- None
- Partial
- Complete

What is the potential for confidentiality compromise?
- None
- Partial
- Complete

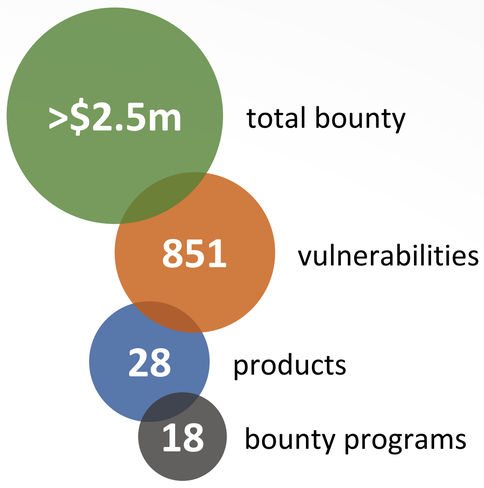
Base metrics are used to compute the base score (0.0 to 10.0)

## Empirical Analysis

**Quantitative** Spearman's Rank Correlation Coefficient ($\rho$)

**Qualitative** Emergent Coding

## Data Set




## Data Sources

hackerone  Chrome Releases

## Programs

THE APACHE SOFTWARE FOUNDATION  OpenSSL  RAILS  php  NGINX  INTERNET BUG BOUNTY

## Quantitative Analysis

**Are severe vulnerabilities awarded higher bounties?**

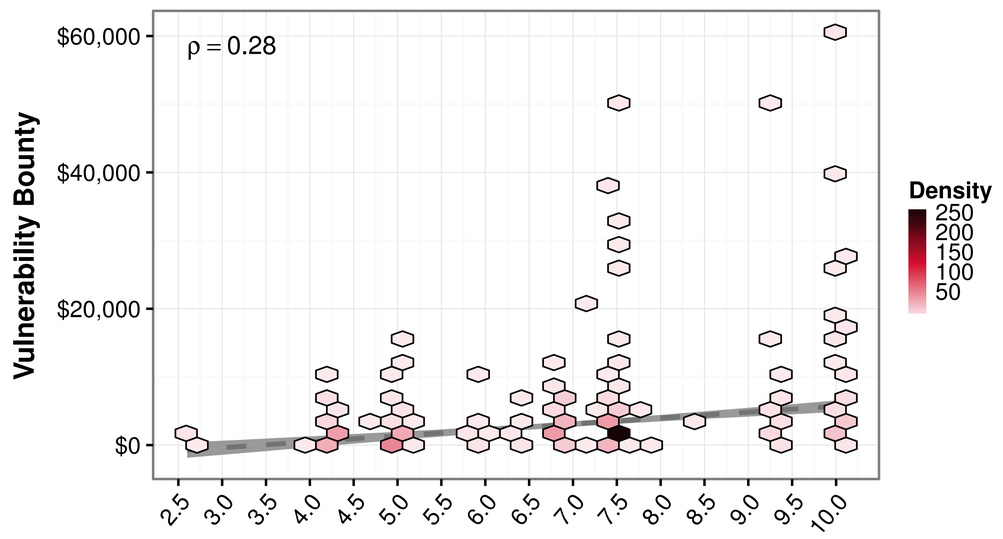



**Figure 1:** Scatterplot of CVSS base score versus bounty

Weak correlation indicates that severe vulnerabilities are not always awarded higher bounties

## Qualitative Analysis

**How do the assessment criteria for bounties differ from those of CVSS?**

**Table 1:** Bounty determination criteria by mention (or omission) in CVSS

| Bounty Determination Criteria (Number of Products) | Calc. | Base | Full |
|---|---|---|---|
| remote vector (14), exploit difficulty (10), denial of service (3), authentication (2), confidentiality (1) | ✓ | ✓ | ✓ |
| unlikely user interaction (5), user confusion (4), configuration (3) | ✗ | ✓ | ✓ |
| overall report quality (16), reproduction code or data (15), fix patch (5), automated exploit (1) | ✗ | ✗ | ✓ |
| panel of project maintainers (20), code execution (16), sandbox (9), specific data, files, or directories (8), xss (7), host environment (5), same-origin policy (4), compounding effects (4), sql-i (4), csrf (3), privilege escalation (3), predefined severity levels (2), compatibility test case (1), firmware (1), kernel (1), patch adherence to coding standards (1), permanence of exploit (1), reliable exploit (1), session management (1), side channels (1), specific versions (1), unvalidated redirects (1) | ✗ | ✗ | ✗ |

22 of the 34 bounty determination criteria not mentioned in CVSS

## Reference

Nuthan Munaiah and Andrew Meneely. 2016. Vulnerability Severity Scoring and Bounties: Why the Disconnect?. In *Proceedings of the 2nd International Workshop on Software Analytics* (SWAN 2016). ACM, New York, NY, USA, 8-14. DOI: https://doi.org/10.1145/2989238.2989239

HOTSOS SYMPOSIUM & BOOTCAMP
HOT TOPICS in the SCIENCE OF SECURITY

***HoTSoS*** *Symposium and Bootcamp*
HOT TOPICS *in the* **SCIENCE OF SECURITY**
APRIL 4-5, 2017 | HANOVER, MARYLAND