Are Vulnerabilities Discovered and Resolved like Other Defects?

Extended Abstract

Patrick J. Morrison
North Carolina State University,
Raleigh, NC, USA
pjmorris@ncsu.edu

Rahul Pandita
Phase Change Software,
Golden, CO, USA
rpandita@phasechange.ai

Xusheng Xiao
Case Western Reserve University,
Cleveland, OH, USA
xusheng.xiao@case.edu

Ram Chillarege
Chillarege Inc.,
Raleigh, NC, USA
info@chillarege.com

Laurie Williams
North Carolina State University,
Raleigh, NC, USA
williams@csc.ncsu.edu

ACM Reference Format:
Patrick J. Morrison, Rahul Pandita, Xusheng Xiao, Ram Chillarege, and Laurie Williams. 2018. Are Vulnerabilities Discovered and Resolved like Other Defects?: Extended Abstract. In *Proceedings of ICSE '18*. ACM, New York, NY, USA, 1 page. https://doi.org/10.1145/3180155.3182553

H.4Information Systems ApplicationsMiscellaneous D.2.8Software EngineeringMetrics[complexity measures, performance measures]

1 ABSTRACT

Context: Software defect data has long been used to drive software development process improvement. If security defects (i.e., vulnerabilities) are discovered and resolved by different software development practices than non-security defects, the knowledge of that distinction could be applied to drive process improvement.
Objective: *The goal of this research is to support technical leaders in making security-specific software development process improvements by analyzing the differences between the discovery and resolution of defects versus that of vulnerabilities.*
Method: We extend Orthogonal Defect Classification (ODC) [1], a scheme for classifying software defects to support software development process improvement, to study process-related differences between vulnerabilities and defects, creating ODC + Vulnerabilities (ODC+V). We applied ODC+V to classify 583 vulnerabilities and 583 defects across 133 releases of three open-source projects (Firefox, phpMyAdmin, and Chrome).
Results: Compared with defects, vulnerabilities are found later in the development cycle and are more likely to be resolved through changes to conditional logic. In Firefox, vulnerabilities are resolved 33% more quickly than defects. From a process improvement perspective, these results indicate opportunities may exist for more efficient vulnerability detection and resolution.

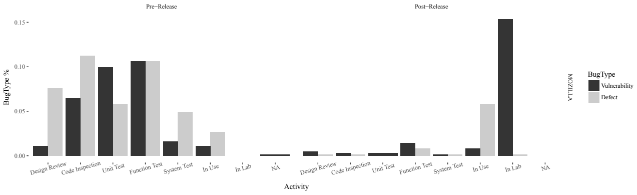

Figure 1: Firefox

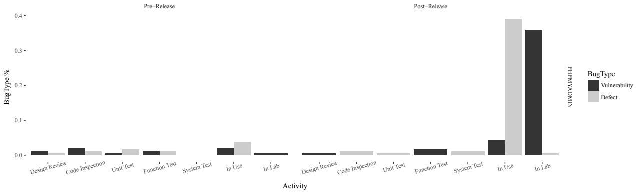

Figure 2: phpMyAdmin

Figures 1 and 2 present the percentage of defects and vulnerabilities found in each Activity for Firefox and phpMyAdmin, ordered from left to right as a timeline, first by pre-release, then by post-release. In these projects, pre-release effort in vulnerability and defect detection correlates with pre-release vulnerability and defect resolution.
Conclusion: We found ODC+V's property of associating vulnerability and defect discovery and resolution events with their software development process contexts helpful for gaining insight into three open source software projects. The addition of the SecurityImpact attribute, in particular, brought visibility into when threat types are discovered during the development process. We would expect use of ODC+V (and of base ODC) periodically over time to be helpful for steering software development projects toward their quality assurance goals.

We give our full report in Morrison et al. [2] [1]

REFERENCES

[1] Ram Chillarege et al. ODC-a 10x for root cause analysis. 2006. Available online at: http://www.chillarege.com/articles/odc-10x-root-cause-analysis.html.
[2] Patrick John Morrison, Rahul Pandita, Xusheng Xiao, Ram Chillarege, and Laurie A. Williams. Are vulnerabilities discovered and resolved like other defects? *Empirical Software Engineering*, pages 1–39, 2017.

[1] https://doi.org/10.1007/s10664-017-9541-1

ICSE '18, May 27-June 3, 2018, Gothenburg, Sweden,

ACM ISBN 978-1-4503-5638-1/18/05.
https://doi.org/10.1145/3180155.3182553