Are Vulnerabilities Discovered and Resolved like Other Defects?

Patrick J. Morrison[†], Rahul Pandita[*], Xusheng Xiao[‡], Ram Chillarege[∓], and Laurie Williams[†]
[†]North Carolina State University, Raleigh, NC, USA
[*]Phase Change Software, Golden, CO, USA
[†]Case Western Reserve University, Cleveland, OH, USA
[∓]Chillarege Inc., Raleigh, NC, USA
pjmorris@ncsu.edu, rpandita@phasechange.ai, xusheng.xiao@case.edu, info@chillarege.com, and williams@csc.ncsu.edu

ABSTRACT

Context: Software defect data has long been used to drive software development process improvement. If security defects (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), 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.

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.

ICSE 2018 Gothenburg, Sweden

Categories and Subject Descriptors

H.4 [**Information Systems Applications**]: Miscellaneous; D.2.8 [**Software Engineering**]: Metrics—*complexity measures, performance measures*

1. PUBLICATION POINTER

Morrison et al. [1] [1] [2]

2. REFERENCES

[1] Patrick J. Morrison, Rahul Pandita, Xusheng Xiao, Ram Chillarege, and Laurie Williams. Are vulnerabilities discovered and resolved like other defects? *Empirical Software Engineering*, 2017.

[1] https://www.springerprofessional.de/en/are-vulnerabilities-discovered-and-resolved-like-other-defects/15071466

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