Engineering Village™

1. **An Investigation into Inconsistency of Software Vulnerability Severity across Data Sources**
Croft, R.; Babar, M.A.; Li, L. **Source:** *2022 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER)*, 338-48, 2022; **ISBN-13:** 978-1-6654-3786-8; **DOI:** 10.1109/SANER53432.2022.00050; **Conference:** 2022 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER), 15-18 March 2022, Honolulu, HI, USA; **Publisher:** IEEE, Piscataway, NJ, USA

Author affiliation:
University of Adelaide, School of Computer Science, Adelaide, SA, Australia
Cyber Security Cooperative Research Centre, Australia
Monash University, Faculty of Information Technology, Melbourne, VIC, Australia

Abstract: Software Vulnerability (SV) severity assessment is a vital task for informing SV remediation and triage. Ranking of SV severity scores is often used to advise prioritization of patching efforts. However, severity assessment is a difficult and subjective manual task that relies on expertise, knowledge, and standardized reporting schemes. Consequently, different data sources that perform independent analysis may provide conflicting severity rankings. Inconsistency across these data sources affects the reliability of severity assessment data, and can consequently impact SV prioritization and fixing. In this study, we investigate severity ranking inconsistencies over the SV reporting lifecycle. Our analysis helps characterize the nature of this problem, identify correlated factors, and determine the impacts of inconsistency on downstream tasks. Our findings observe that SV severity often lacks consideration or is underestimated during initial reporting, and such SVs consequently receive lower prioritization. We identify six potential attributes that are correlated to this misjudgment, and show that inconsistency in severity reporting schemes can severely degrade the performance of downstream severity prediction by up to 77%. Our findings help raise awareness of SV severity data inconsistencies and draw attention to this data quality problem. These insights can help developers better consider SV severity data sources, and improve the reliability of consequent SV prioritization. Furthermore, we encourage researchers to provide more attention to SV severity data selection. (0 refs.) **Inspec controlled terms:** decision making - public domain software - road safety - security of data

Uncontrolled terms: SV severity data selection - Software Vulnerability severity assessment - vital task - triage - SV severity scores - patching efforts - difficult manual task - subjective manual task - independent analysis - conflicting severity rankings - severity assessment data - SV prioritization - severity ranking - SV reporting lifecycle - downstream tasks - initial reporting - lower prioritization - severity reporting schemes - downstream severity prediction - SV severity data inconsistencies - data quality problem - severity data sources

Classification Code: C6130S Data security - C1160 Combinatorial mathematics - C7330 Biology and medical computing

IPC Code: G06F21/00 - G16B

Treatment: Practical (PRA)

Database: Inspec