1. **SSPCatcher: Learning to catch security patches**

Sawadogo, Arthur D.; Bissyandé, Tegawendé F.; Moha, Naouel; Allix, Kevin; Klein, Jacques; Li, Li; Le Traon, Yves **Source:** *Empirical Software Engineering*, v 27, n 6, November 2022; **ISSN:** 13823256, **E-ISSN:** 15737616; **DOI:** 10.1007/s10664-022-10168-9; **Article number:** 151; **Publisher:** Springer

Author affiliation:
Université du Québec à Montréal, Montréal; QC, Canada
SnT, University of Luxembourg, 2 Av. de l'Universite, Esch-sur-Alzette; 4365, Luxembourg
Monash University, Melbourne; VIC, Australia

Abstract:

Timely patching (i.e., the act of applying code changes to a program source code) is paramount to safeguard users and maintainers against dire consequences of malicious attacks. In practice, patching is prioritized following the nature of the code change that is committed in the code repository. When such a change is labeled as being security-relevant, i.e., as fixing a vulnerability, maintainers rapidly spread the change, and users are notified about the need to update to a new version of the library or of the application. Unfortunately, oftentimes, some security-relevant changes go unnoticed as they represent silent fixes of vulnerabilities. In this paper, we propose SSPCatcher, a Co-Training-based approach to catch security patches (i.e., patches that address vulnerable code) as part of an automatic monitoring service of code repositories. Leveraging different classes of features, we empirically show that such automation is feasible and can yield a precision of over 80% in identifying security patches, with an unprecedented recall of over 80%. Beyond such a benchmarking with ground truth data which demonstrates an improvement over the state-of-the-art, we confirmed that SSPCatcher can help catch security patches that were not reported as such.
(54 refs.)

Main Heading: Network security

Uncontrolled terms: Automatic monitoring - Co-training - Code changes - Different class - Ground truth data - Malicious attack - Monitoring services - Program source codes - Security patches - State of the art

Classification Code: 723 Computer Software, Data Handling and Applications

Funding details: Number: -, Acronym: ISM, UQAM, Sponsor: Institut des Sciences Math&eacute;matiques, Universit&eacute; du Qu&eacute;bec &agrave; Montr&eacute;al;

Database: Compendex