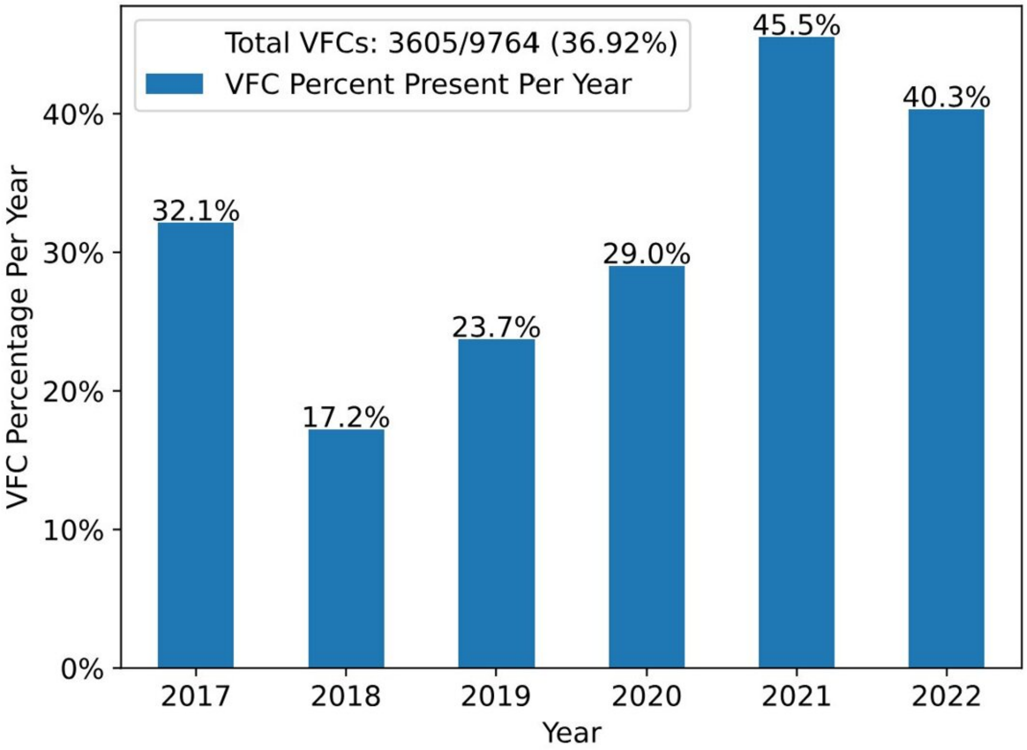
New tool pinpoints security fixes in open-source software updates

May 9 2024, by Matt Shipman



63.1% of GHSA security advisories are missing their patch link based on a snapshot taken through 2022. Credit: *arXiv* (2023). DOI: 10.48550/arxiv.2311.01532

Researchers have demonstrated a new tool that analyzes open-source software updates to specify which sections of code are being modified to address recently identified security vulnerabilities. The tool, called VFCFinder, should make it faster and easier for programmers to determine which security updates are necessary to prevent vulnerabilities without having to make unnecessary changes.

"Updates to open-source computer code often include changes designed to address security vulnerabilities," says William Enck, co-author of a paper on the work and a professor of computer science at North Carolina State University. "But many programs that use open-source code are not affected by any given vulnerability—and accepting unnecessary updates can create programming challenges of its own. That makes it important for programmers to understand which vulnerability updates will actually make their programs more secure."

Open-source software is software that is issued under a license that allows users to study and modify the software's code. It is used in a wide variety of applications by users ranging from individuals to large corporations.

Existing processes for notifying the public about security vulnerabilities in open-source software let users know that a vulnerability exists and that users should adopt an updated version of the software which addresses the vulnerability. However, in modern coding, many developers create new programs that rely on a library of pieces of code, each of which performs a specific function. And if one of the pieces of code you're relying on needs to be updated, that could cause problems for the larger program.

"This makes it important for programmers using open-source code libraries to understand the nature of each vulnerability, including which specific sections of computer code are responsible for the vulnerability," says Trevor Dunlap, first author of the paper and a Ph.D. student at NC State. "Depending on the nature of the vulnerability, many programmers may not need to perform the update. But most security advisories don't make clear exactly what the problem was—only that a problem was identified, and an update would fix it."

"To provide some context for the challenge here, there are tens to hundreds of security advisories announced each day; there were more than 29,000 in 2023," Enck says. "Every time software is updated, it includes lots of different software modifications, called commits, only some of which may be relevant to a program that uses that software.

"Right now, most programmers make use of source composition analysis (SCA) services that employ coders to identify the nature of these updates and which pieces of code have been modified to address vulnerabilities," Enck says. "Programmers can then use that information to make decisions about whether to run relevant updates. In short, this requires a lot of people to spend a lot of time poring over code to identify exactly what section of code is responsible for each vulnerability and which types of programs likely need to run the update."

"VFCFinder is used to identify the specific changes that are mostly likely to be responsible for fixing a given vulnerability," says Dunlap. "In other words, VFCFinder makes it much easier for SCA services to identify the affected sections of code. And that, in turn, helps programmers make decisions about whether to update the open-source code they're using in their programs."

To test VFCFinder, the researchers ran it against thousands of vulnerabilities where the commits responsible for fixing each vulnerability were well established.

"VFCFinder was able to identify the five most likely commits with 96.6% accuracy," Dunlap says. "And it had 80% accuracy at precisely identifying the commit that fixed the vulnerability. The previous state-of-the-art techniques had 44% accuracy at precisely identifying the relevant commit."

The researchers then tested VFCFinder against several hundred security advisories for which the relevant commit had not been identified.

"The numbers were pretty much the same when looking at these advisories," Dunlap says. "Actually, the results were even better, as VFCFinder was able to identify the relevant commit 81% of the time precisely. And our results were accepted into the GitHub Security Advisory database."

"Ultimately, our goal is to reduce security risks associated with the widespread use of open-source software," says Enck. "We're optimistic that VFCFinder can help make SCA services more efficient, strengthening a critical piece of the software supply chain."

VFCFinder is an open-source tool and can be found on GitHub.

The study is published on the *arXiv* preprint server.

The paper will be presented at the ACM ASIA Conference on Computer and Communications Security, being held July 1-5 in Singapore. The paper was co-authored by Elizabeth Lin, a Ph.D. student at NC State, and Brad Reaves, an associate professor of computer science at NC State.

More information: Trevor Dunlap et al, VFCFinder: Seamlessly Pairing Security Advisories and Patches, *arXiv* (2023). DOI: 10.48550/arxiv.2311.01532

GitHub: github.com/s3c2/vfcfinder

Provided by North Carolina State University

Citation: New tool pinpoints security fixes in open-source software updates (2024, May 9) retrieved 29 June 2024 from https://techxplore.com/news/2024-05-tool-source-software.html