NTT Security Holdings

November 15, 2024

<Topics>

A new fuzzing automation method to significantly enhance the detection efficiency of software bugs and vulnerabilities

~Eliminating the preparation tasks for launcher programs and input data~

NTT Corporation (hereinafter "NTT") and NTT Security Holdings Corporation (hereinafter "NTT Security") will present a new fuzzing method at the international conference “CODE BLUE 2024”. This method automates the various tasks required for fuzzing, a security-focused software test, enabling efficient fuzzing of a wide variety of software. Using this method, we have discovered numerous bugs and vulnerabilities in Ubuntu’s Debian packages. We anticipate that this research result will contribute to enhancements in NTT Group’s services and security.

“CODE BLUE 2024” is an industry-focused cybersecurity conference held in Japan, with only 24 out of over 350 submissions were accepted this year, making it a highly competitive conference. Our acceptance to this conference signifies that this research represents a leading achievement in the field and will garner significant attention from researchers and practitioners in this field.

Research Results

Our research makes application of fuzzing fully automatic for a wide variety of software. Fuzzing is a security testing technique which involves providing a wide variety of mutated inputs to the test target to induce crashes and identify flaws that could lead to vulnerabilities. Fuzzing has gained significant attention in recent years because many of the vulnerabilities were discovered using this technique.
Traditionally, fuzzing required manual preparation of the program to launch the test target, along with the input data and files. With our method, we have succeeded in automating these manual

operations by monitoring the build/test process of the target software package and automatically collecting the required information for fuzzing. This enabled fuzzing to be applied to a wide variety of software, including small projects that traditionally could not devote a lot of resources to security testing. Using this method, we fuzzed Debian packages in Ubuntu 23.10 and discovered 64,658 crashes, 1,186 bugs, and 5 vulnerabilities in 265 packages. This result has led to the publication of CVEs and security advisories.

Contact Information
NTT Security Holdings Corporation
makoto.iwamura@security.ntt