2024 年 11 月 15 日

<Topics>

ソフトウェアのバグや脆弱性の検出効率を飛躍的に向上させる ファジング自動化技術を創出

～検査対象を起動するプログラムや入力となるデータの準備作業を解消～

日本電信電話株式会社（以下、「NTT」）と NTT セキュリティホールディングス株式会社（以下、「NTT セキュリティ」）は、国際会議「CODE BLUE 2024」で新しいファジング技術を発表します。本技術は、ソフトウェアセキュリティのテストの 1 つであるファジングを行うために必要だった多くの手作業を自動化することで、多様なソフトウェアへの効率的なファジングを実現します。この技術を用いて、Ubuntu の Debian パッケージから多くのバグと脆弱性を発見しました。これにより、ＮＴＴグループのサービス高度化とセキュリティの向上が期待されます。

「CODE BLUE 2024」は、日本で開催されるサイバーセキュリティ分野における産業系国際会議で、今年は 350 以上の応募の中から、わずか 24 件の採録となった競争率の高い会議です。本会議への採択は、サイバーセキュリティ分野のトップレベルの成果として認められたことを意味し、当該分野における研究者や実務者から大きな注目を集めます。

【研究成果】

本技術は、ファジングを様々なソフトウェアに対して全自動で適用可能にします。ファジングとは、多様に変化させた入力を検査対象へ与え、クラッシュを引き起こさせることで脆弱性の元となるプログラム上の欠陥を見つけるセキュリティテスト手法です。近年、非常に多くの脆弱性がこのファジングにより発見されていることで注目を集めています。

従来、ファジングを行うためには、検査対象を起動するプログラムや検査対象への入力となるデータやファイルの準備を手作業で実施していました。本技術では、検査対象ソフトウェアのソフトウェアパッケージのビルド・テストプロセスを監視し、ファジングに必

要な情報を自動収集することで、これら手作業を自動化することに成功しました。これにより、従来はセキュリティテストに多くのリソースをかけられなかった小規模なプロジェクトを含む多様なソフトウェアへのファジングの適用を可能にしました。本技術を利用し、Ubuntu 23.10 の Debian パッケージを対象にファジングを実施し、265 のパッケージから 64,658 件のクラッシュ、1,186 件のバグを検出し、5 件の脆弱性を特定しました。この成果は CVE・アドバイザリの発行にもつながりました。

【お問い合わせ先】
NTT セキュリティホールディングス株式会社
makoto.iwamura@security.ntt