softScheck

sCFF – softScheck Cloud Fuzzing Framework

Veröffentlichung des Fuzzing Framework Tools sCFF auf Github

Fuzzing ist eine Methode um die Robustheit einer Software zu testen. Dazu wird ein Zielprogramm immer wieder mit unterschiedlichen Eingabedaten ausgeführt. Treten Anomalien bei der Ausführung auf (Absturz, Hänger etc.), so wird dies vom Fuzzer erkannt. Diese Anomalien sind oftmals Buffer Overflows und lassen sich von einem Angreifer ausnutzen. Es ist Ratsam Produkte mit Fuzzern zu testen um automatisiert ein großes Spektrum von möglichen Fehlern zu identifizieren.

In Zeiten von Infrastructure as a Service (IaaS) ist es kein Problem mehr, Software, wie beispielsweise einen Fuzzer, in der Cloud laufen zu lassen. Die Cloud bietet viele Vorteile gegenüber klassischem Fuzzing. Die haben auch größere Unternehmen wie Microsoft oder Google erkannt und fuzzen daher in der Cloud. softScheck hat sich ebenfalls entschlossen in der Cloud zu Fuzzen und ein Framework entwickelt, welches Fuzzing in der Cloud erleichtert.

Das Fuzzing Framework sCFF – softScheck Cloud Fuzzing Framework, wird hiermit der Allgemeinheit zugänglich gemacht. Interessierte können den Quellcode auf Github einsehen.

sCFF unterstützt den Software Tester bei allen Phasen des Fuzzings inklusive deployment, sowie das analysieren der Funde. Aktuell unterstützt sCFF die Amazon Cloud und nutzt AFL zur Erstellung der Fuzzingdaten. Entwickler können Module für andere Cloud Plattformen sowie Fuzzer hinzufügen.

Die Software ist aktuell noch in der Alphaphase, wird bei softScheck jedoch bereits erfolgreich eingesetzt. So konnten wir unter anderem eine Sicherheitslücke in tcpdump identifizieren. Weitere Informationen und Anweisungen, wie auch Sie Sicherheitslücken mit sCFF finden können sind auf unserem Blog unter https://www.softscheck.com/en/identifying-security-vulnerabilities-with-cloud-fuzzing/ nachzulesen.

Der eine detaillierte Abhandlungen über die Vor- und Nachteile von Cloud Fuzzing bietet folgendes Paper:
https://www.softscheck.com/publications/Pohl_Kirsch_scff_paper_170405.pdf

Sicherheit, IT, IT-Sicherheit, Informationssicherheit, Cloud Fuzzing, sCFF, Dynamic Analysis, Distributed Fuzzing, AWS, AFL, Fuzzing