Black Duck Newsroom

Synopsys Fuzzing Report Identifies IoT and Industrial Control Systems Software as Most Vulnerable to Exploits

Analysis of 4.8 Billion Fuzz Tests Identified 6.6 Seconds as the Average Time to First Failure for the Least Mature Protocol

Disclaimer: The Synopsys Software Integrity Group is now Black Duck®. Click here to learn more.

MOUNTAIN VIEW, Calif., Aug 9, 2017 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS), today released its fuzzing report, which provides deep analysis on potential zero-day exploits in the open source protocols and common file formats used across six key industries, including automotive, financial services, government, healthcare, industrial control systems, and Internet of Things (IoT). The results stem from more than 4.8 billion fuzz tests conducted by Synopsys' customers in 2016 using the Defensics® Fuzz Testing solution. Download the full copy of the Synopsys State of Fuzzing 2017 report.

"Fuzz testing is a powerful component of the Synopsys Software Integrity Platform to uncover zero-day vulnerabilities and help organizations protect their software," said Andreas Kuehlmann, senior vice president and general manager for the Synopsys Software Integrity Group. "By analyzing such a large data set from our customers, the Synopsys fuzzing report provides visibility into unknown, hard-to-find vulnerabilities and highlights where security teams should look to improve the quality and security of their software."

Major findings of the Synopsys State of Fuzzing 2017 include:

- The overall average time to first failure (TTFF) — the first instance when a protocol crash is recorded — was 1.4 hours. In the case of more mature protocols, the length of time is in hours. But with less mature protocols, that time could be as short as a few seconds, indicating a higher likelihood of exploitable vulnerabilities.
- The least mature protocol tested in 2016 was IEC-61850 MMS (ICS). This is a niche protocol used in IoT and industrial control systems. The average TTFF for IEC-61850 MMS was 6.6 seconds.
- The most mature protocol tested in 2016 was TLS client (Core IP). This is commonly used for secure web browsing including online banking and e-commerce. The average TTFF for TLS client was 9 hours.

According to a recent Forrester Research report, "Security pros have applied fuzz testing and application hardening tools on web applications for many years. However, these tools are finding new footholds in the IoT market, where applications are hard to crawl with traditional prerelease testing tools like DAST and face the same tampering threats as mobile applications. As IoT applications become more prevalent, expect fuzz testing and application hardening tools to have a rebirth."[1]

The Synopsys Fuzz Testing product was used to identify the infamous Heartbleed vulnerability OpenSSL, which had gone unidentified for more than two years and impacted more than 500,000 websites. The product uncovers hidden, unknown vulnerabilities and helps organizations improve software security with advanced test suites for 250+ standard network protocols, file formats, and other interfaces. It not only uncovers dangerous unknown

vulnerabilities, but also provides expert remediation advice to help organizations future-proof the software they rely on. See more details about Synopsys' software security products.

About the Synopsys Software Integrity Platform

Synopsys offers the most comprehensive solution for building integrity—security and quality—into the software development lifecycle and supply chain. The Software Integrity Platform unites leading testing technologies, automated analysis and experts to create a robust portfolio of products and services. This portfolio enables companies to develop customized programs for detecting and remediating defects and vulnerabilities early in the development process, minimizing risk and maximizing productivity. Synopsys, a recognized leader in Application Security Testing (AST), is uniquely positioned to adapt and apply best practices to new technologies and trends such as IoT, DevOps, CI/CD, and the Cloud. For more information, go to www.synopsys.com/software.

About Synopsys

Synopsys, Inc. (Nasdaq: SNPS) is the Silicon to Software™ partner for innovative companies developing the electronic products and software applications we rely on every day. As the world's 15th largest software company, Synopsys has a long history of being a global leader in electronic design automation (EDA) and semiconductor IP and is also growing its leadership in software security and quality solutions. Whether you're a system-on-chip (SoC) designer creating advanced semiconductors, or a software developer writing applications that require the highest security and quality, Synopsys has the solutions needed to deliver innovative, high-quality, secure products. Learn more at www.synopsys.com.

1. "TechRadar™: Application Security, Q3 2017", Forrester Research, Inc., July 6, 2017

Editorial Contacts:
Simone Souza
Synopsys, Inc.
650-584-6454
simone@synopsys.com

SOURCE Synopsys, Inc.

---

https://news.blackduck.com/2017-08-09-Synopsys-Fuzzing-Report-Identifies-IoT-and-Industrial-Control-Systems-Software-as-Most-Vulnerable-to-Exploits