Beating hackers at bug hunting

July 14 2022, by John Maxwell, Tanya Petersen

Credit: Pixabay/CC0 Public Domain

An innovative new collaboration between EPFL's HexHive Laboratory and Oracle has developed automated, far-reaching technology in the ongoing battle between IT security managers and attackers, hoping to find bugs before the hackers do.

On the 9th of December 2021 the world of IT security went into a state of shock. Before its developers even knew it, the log4j application—part of the Apache suite used on most web servers—was being exploited by hackers, allowing them to take control of servers and data centers all over the world.

The Wall Street Journal reported news that nobody wanted to hear: "U.S. officials say hundreds of millions of devices are at risk. Hackers could use the bug to steal data, install malware or take control."

93% of the world's cloud services affected

One estimate stated that the vulnerability affected 93% of enterprise cloud environments. At EPFL, all IT administrators were sent instructions to patch their server software immediately. Even Oracle Corporation, world leaders in information security, had to send out a distress call: "Due to the severity of this vulnerability and the publication of exploit code on various sites, Oracle strongly recommends that customers apply the updates provided by our Security Alert as soon as possible."

Victims of the log4j bug included the Belgian Ministry of Defense, the U.K.'s National Health Service and a range of financial trading platforms. So, what have corporations like Oracle done to try to prevent an incident like this occurring again?

In fact, Oracle had already been working against this kind of vulnerability before the outbreak, including a collaboration with Professor Mathias Payer of EPFL's HexHive lab.

"We had already covered similar kinds of program analysis, and had worked on cloud security as part of EPFL's EcoCloud Center," explained Payer, "but we had not approached bugs like this. Then we got to work

with Oracle Labs which provided funding via a gift. François Gauthier and Kostyantyn Vorobyov, two Oracle researchers, introduced us to the complex technical issues that they were facing and we worked together to develop a platform for discovering these kinds of vulnerabilities."

"People have been attempting to find and exploit vulnerabilities in server code, including Oracle's, for years, either intent on gaining some kind of direct advantage or to earn money by submitting bug reports. Either way, these are dedicated, manual attacks. In these manual attacks, the analyst thoroughly analyzes the source code of the target and then painstakingly crafts their attack. What we have developed is a mechanism that automates that process, and allows Oracle to get ahead of the attackers," he continued.

Eight moves ahead, like a chess grandmaster

"In addition to this, the bugs that we are finding can be much more complex than the ones that experts are finding manually. Most analysts are trained to search to a depth of two manipulations. Our platform can do a search to a depth of up to eight manipulations," said Payer.

The battle between IT security managers and attackers is one where the defenders hope to find bugs before the attackers do and now security managers have one key advantage when it comes to using HexHive's platform. "Although our tool is neutral, that is, it can be used by both attackers and defenders, developers have full access to, and understanding of, their own code, which gives them a huge advantage over a hacker when it comes to interpreting the results. They therefore have a very good chance of finding weak points before the attacker."

Plans are underway to set up internships for HexHive researchers at Oracle Corporation, a win-win for both the company and EPFL. Oracle will have people who actually developed some of the code on site,

making it easier to integrate the platform into their pipeline. At the same time, the placements will provide great experience for EPFL researchers and HexHive's prototype will remain open source with bug reports all published."

So long as information technology is around, the battle between security managers and hackers will rage on. Thanks to its collaboration with HexHive, Oracle will be able to keep one step ahead of the aggressor: faster, higher, stronger.

Provided by Ecole Polytechnique Federale de Lausanne