Computer security experts scramble to fix 'vulnerability of the decade'

December 22 2021, by Gopal Ratnam

Credit: CC0 Public Domain

Criminals, cyber spies, and hackers around the world are launching thousands of attempts every hour to exploit a flaw in a widely used logging software as cybersecurity experts are scrambling to close the

loophole and prevent catastrophic attacks.

In early December, a security researcher at Chinese online retailer Alibaba discovered and reported the software flaw in a widely used tool called log4j. The open-source tool is a Java-based library developed by Apache that software developers use to track activity within an application.

Every time anyone on the internet connects to a site, a cloud-service provider, or others, the company managing the site or the service captures data about the activity and stores it in a log. Hackers are now attempting to break into such logs and launch attacks.

"We have kind of what I call a threefold problem here," said Steve Povolny, principal engineer and head of advanced threat research at McAfee Enterprise. "The simplicity of the attack, the ubiquity of vulnerable installed base, and the wide availability of exploit code really combine to make this …maybe the vulnerability of the decade."

Although Apache has offered a patch to fix the flaw, companies and government agencies use many versions of the log4j tool and are trying to figure out which fix works with what version, Povolny said. But as of late last week, security researchers have identified that a fix known as version 2.16 "effectively solves the problem," he said.

Nevertheless, as companies and government agencies around the world attempt to fix the problem there's "no question that this has been and is going to continue to be further weaponized," Povolny said.

The widespread vulnerability marks a bookend to a year notable for significant cyber and ransomware attacks. At the start of 2021 the world began to grapple with the consequences of a sophisticated Russian attack on SolarWinds, a software management company, which was discovered

in December 2019. The attack exposed dozens of U.S. agencies and thousands of companies to potential exploitation by Russian intelligence services.

In the months since, ransomware attacks crippled pipeline operator Colonial Pipeline and major food processor JBS Foods in addition to universities, cities and towns.

Required reporting of hacks

The Biden administration has launched a series of efforts to curb the spread of ransomware, and Congress has debated whether to require reporting of attacks as well as mandatory adoption of basic cyber hygiene measures by private companies and government agencies.

The log4J vulnerability opens a new front in worldwide cyberattacks, and experts are worried that criminals and others could launch a so-called worm, which is a malicious software code that self-propagates and spreads across the world, Povolny said.

Late last week Microsoft warned that it was seeing "mass scanning" of computer systems, potentially by both attackers as well as security researchers trying to race ahead of the bad guys.

As security researchers try to identify systems that have been compromised, attackers are staying one step ahead by obfuscating their attacks, Microsoft said in a blog post.

Microsoft said that attackers had launched a ransomware labeled Khonsari that targets servers running the Minecraft video game, and advised players to download the latest version of the game software to plug the loophole.

Nation-state backed hackers from China, Iran, North Korea, and Turkey are trying to exploit the log4jloophole, Microsoft said.

An Iranian hacker group known as Phosphorus "has been deploying ransomware, acquiring and making modifications of the log4j exploit," Microsoft said." The group is likely to have "operationalized these modifications."

A Chinese hacking group labeled Hafnium "has been observed utilizing the vulnerability to attack virtualization infrastructure to extend their typical targeting," Microsoft said.

The Cybersecurity and Infrastructure Security late last week issued an emergency order asking all federal agencies to patch log4j vulnerabilities "immediately."

"The log4j vulnerabilities pose an unacceptable risk to federal network security," CISA Director Jen Easterly said in a statement. "CISA has issued this emergency directive to drive federal civilian agencies to take action now to protect their networks, focusing first on internet-facing devices that pose the greatest immediate risk."

Povolny compared the rush to patch the software flaw to the drive to vaccinate people against COVID-19.

"If you get a high enough percentage of people vaccinated against or patched against" the log4j flaw "you have a much lower likelihood of impact for a virus being replicated or a worm being able to actually spread itself here," Povolny said.