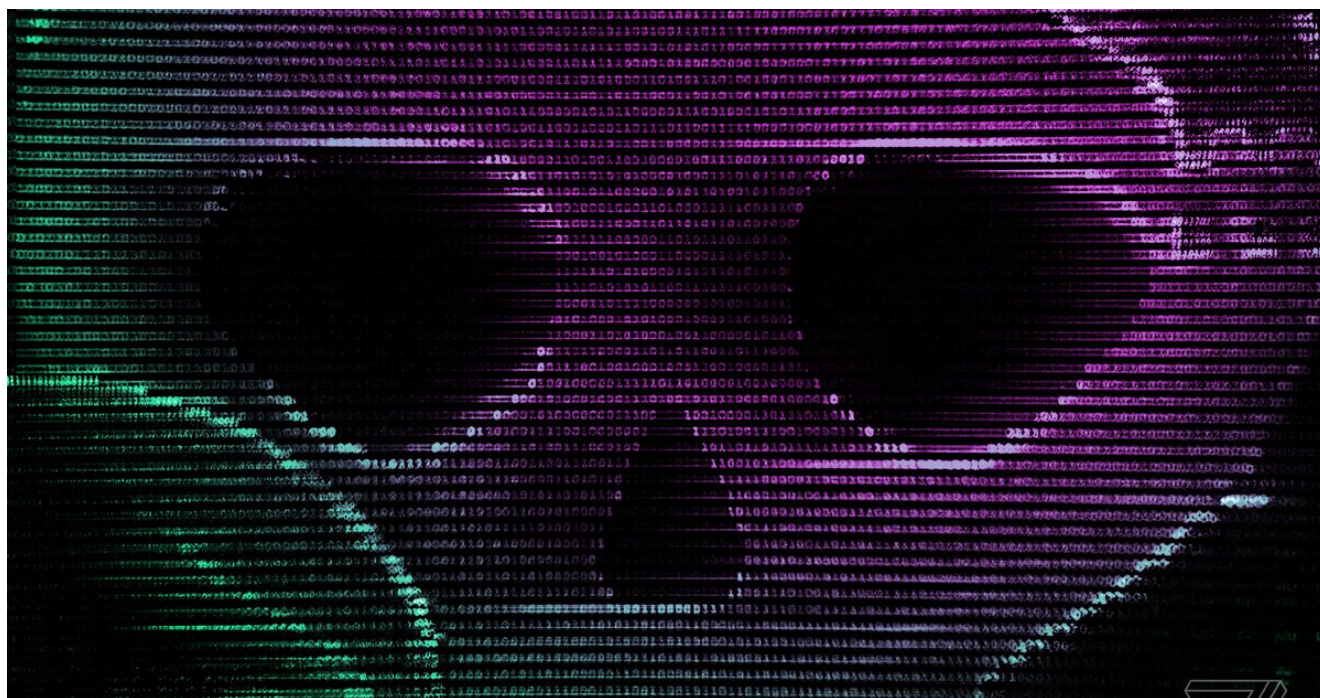


'Extremely bad' vulnerability found in widely used logging system



Security teams at companies large and small are scrambling to patch a previously unknown vulnerability called Log4Shell, which has the potential to let hackers compromise millions of devices across the internet.

If exploited, the vulnerability allows remote code execution on vulnerable servers, giving an attacker the ability to import malware that would completely compromise machines.

The vulnerability is found in log4j, an open-source logging library used by apps and services across the internet. Logging is a process where applications keep a running list of activities they have performed which can later be reviewed in case of error. Nearly every network security system runs some kind of logging process, which gives popular libraries like log4j an enormous reach.

"When I look back over the last 10 years, there are only two

other exploits I can think of with a similar severity"

Marcus Hutchins, a prominent security researcher best known for halting the global WannaCry malware attack, noted online that millions of applications would be affected. "Millions of applications use Log4j for logging, and all the attacker needs to do is get the app to log a special string," Hutchins said in a tweet.

The exploit was first seen on sites hosting *Minecraft* servers, which discovered that attackers could trigger the vulnerability by posting chat messages. A tweet from security analysis company GreyNoise reported that the company has already detected numerous servers searching the internet for machines vulnerable to the exploit.

A blog post from application security company LunaSec claimed that gaming platform Steam and Apple's iCloud had already been found to be vulnerable. Neither Valve nor Apple immediately responded to a request for comment.

To exploit the vulnerability, an attacker has to cause the application to save a special string of characters in the log. Since applications routinely log a wide range of events – such as messages sent and received by users, or the details of system errors – the vulnerability is unusually easy to exploit and can be triggered in a variety of ways.

"This is a very serious vulnerability because of the widespread use of Java and this package log4j," Cloudflare CTO John Graham-Cumming told *The Verge*. "There's a tremendous amount of Java software connected to the internet and in back-end systems. When I look back over the last 10 years, there are only two other exploits I can think of with a similar severity: Heartbleed, which allowed you to get information from servers that should have been secure, and Shellshock, which allowed you to run code on a remote machine."

However, the diversity of applications vulnerable to the

exploit, and range of possible delivery mechanisms, mean that firewall protection alone does not eliminate risk. Theoretically, the exploit could even be carried out physically by hiding the attack string in a QR code that was scanned by a package delivery company, making its way into the system without having been sent directly over the internet.

An update to the log4j library has already been released to mitigate against the vulnerability, but given the time taken to ensure that all vulnerable machines are updated, Log4Shell remains a pressing threat.

<https://www.theverge.com/2021/12/10/22828303/log4j-library-vulnerability-log4shell-zero-day-exploit>