

Logging Library for Millions of Apps is a Serious Vulnerability

Millions of devices are susceptible to attacks due to the vulnerability known as Log4Shell in the open-source log library Log4j. The Verge points out that apps and services keep the track of every event during their operation, giving the ability to examine how their program is running and to discover the reason for the error if there are errors. Log4j happens to be an extremely popular and widely used logging library, and even popular cloud services like Steam and iCloud, as well as apps like Amazon, Twitter and Minecraft are believed to be vulnerable to attacks that exploit Log4Shell.

According to Ars Technica, it first came to light after Minecraft websites started reporting about a vulnerability allowing hackers to execute malicious code in the game. It was discovered shortly after, though, that the problem doesn't affect Minecraft only. Marcus Hutchins, a security researcher who stopped the spread from WannaCry malware identified the vulnerability as "extremely serious" because millions of applications use Log4j to log.

The threat of malicious actors using it remotely to execute code on servers and direct them to download and execute malware that compromises the data of companies and individuals. Additionally, it's quite easy to exploit and could be triggered by posting messages. Hutchins stated that in the case of Minecraft, attackers were capable of executing code remotely through the posting of a message in the chatbox. LunaSec is an app security firm, declared that the vulnerability in Apple's servers is done by simply changing the iPhone's name.

MINECRAFT SERVERS

Log4j has already issued an update to fix the vulnerability and affected services such as Minecraft and Cloudflare have already issued patches to protect users. Log4j users who manage their own networks might need to update their systems as quickly as possible if possible.