arstechnica.com

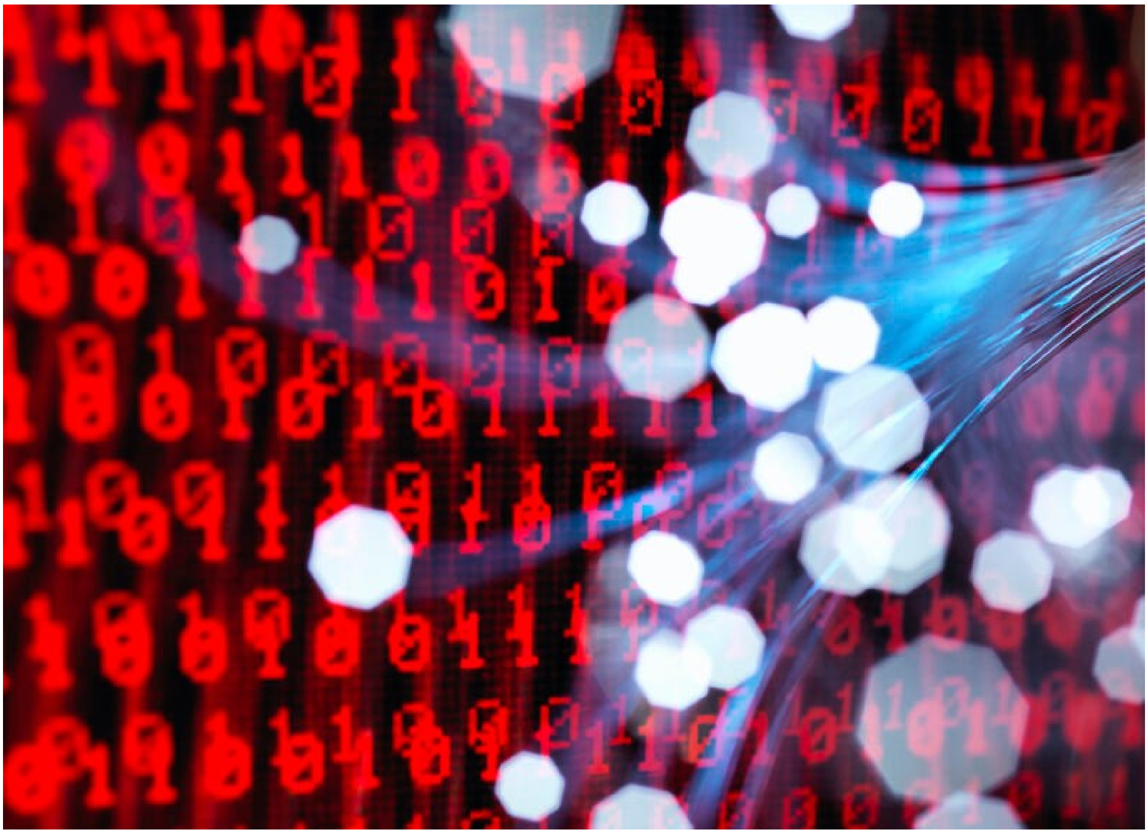
Zero-day in ubiquitous Log4j tool poses a grave threat to the Internet

Dan Goodin - 12/10/2021, 5:35 AM

7-8 minutos

Java (de)serialization badness —

Minecraft is the first, but certainly not the last, app known to be affected.



Getty Images

Exploit code has been released for a serious code-execution vulnerability in Log4j, an open source logging utility that's used in countless apps, including those used by large enterprise organizations, several websites reported last Thursday.

Word of the vulnerability first came to light on sites catering to users of *Minecraft*, the best-selling game of all time. The sites warned that hackers could execute malicious code on servers or clients running the Java version of *Minecraft* by manipulating log messages, including from things typed in chat messages. The picture became more dire still as Log4j was identified as the source of the vulnerability, and exploit code was discovered posted online.

A big deal

“The *Minecraft* side seems like a perfect storm, but I suspect we are going to see affected applications and devices continue to be identified for a long time,” HD Moore, founder and CTO of network discovery platform Rumble, said. “This is a big deal for environments tied to older Java runtimes: Web front ends for various network appliances, older application environments using legacy APIs, and *Minecraft* servers, due to their dependency on older versions for mod compatibility.”

Reports are already surfacing of servers performing Internet-wide scans in attempts to locate vulnerable servers.

> @GreyNoise is currently seeing 2 unique IP's scanning the internet for the new Apache Log4j RCE vulnerability (No CVE assigned yet).
> A tag to track this activity on https://t.co/QckU3An40q will be made available shortly and linked as a reply when released.
>
> — remy🐀 (@_mattata) December 10, 2021

Log4j is incorporated into a host of popular frameworks, including Apache Struts2, Apache Solr, Apache Druid, and Apache Flink. That means that a dizzying number of third-party apps may also be vulnerable to exploits of the same high severity as those threatening *Minecraft* users.

At the time this post went live, there wasn’t much known about the vulnerability. One of the few early sources providing a tracking number for the vulnerability was Github, which said it's CVE-2021-44228. Security firm Cyber Kendra on late Thursday reported a Log4j RCE Zero day being dropped on the Internet and concurred with Moore that “there are currently many popular systems on the market that are affected.”

The Apache Foundation has yet to disclose the vulnerability, and representatives there didn't respond to an email. This Apache page does acknowledge the recent fixing of a serious vulnerability. Moore and other researchers said the Java deserialization bug stems from Log4j making network requests through the JNDI to an

LDAP server and executing any code that's returned. The bug is triggered inside of log messages with use of the ${} syntax.

Additional reporting from security firm LunaSec said that Java versions greater than 6u211, 7u201, 8u191, and 11.0.1 are less affected by this attack vector, at least in theory, because the JNDI can't load remote code using LDAP. Hackers may still be able to work around this by leveraging classes already present in the target application. Success would depend on whether there are any dangerous gadgets in the process, meaning newer versions of Java may still prevent code execution but only depending on the specifics of each application.

LunaSec went on to say that cloud services from Steam and Apple iCloud have also been found to be affected. Company researchers also pointed out that a different high-severity vulnerability in struts led to the 2017 compromise of Equifax, which spilled sensitive details for more than 143 million US consumers.

Cyber Kendra said that in November the Alibaba Cloud security team disclosed a vulnerability in Log4j2—the successor to Log4j—that stemmed from recursive analysis functions, which attackers could exploit by constructing malicious requests that triggered remote code execution. The firm strongly urged people to use the latest version of Log4j2 available here.

What it means for *Minecraft*

The Spigot gaming forum said that *Minecraft* versions 1.8.8 through the most current 1.18 release are all vulnerable, as did other popular game servers such as Wynncraft. Gaming server and news site Hypixel, meanwhile, urged *Minecraft* players to take extra care.

“The issue can allow **remote access to your computer through the servers you log into**,” site representatives wrote. “That means any public server you go onto creates a risk of being hacked.”

Reproducing exploits for this vulnerability in *Minecraft* aren’t straightforward because success depends not only on the *Minecraft* version running but also on the version of the Java framework the *Minecraft* app is running on top of. It appears that older Java versions have fewer built-in security protections that make exploits easier.

On Friday, *Minecraft* rolled out a new game version that fixes the vulnerability.

"We are aware of recent discussions regarding a public exploitation of a Log4j remote code execution vulnerability affecting various industry-wide Apache products," Microsoft said in a statement. "We’ve taken steps to keep our customers safe and protected, which includes rolling out a fix that blocks this issue for Java Edition 1.18.1. Customers who apply the fix are protected.”

For those who can't install the fix right away, Spigot and other sources have said that adding the JVM flag `-Dlog4j2.formatMsgNoLookups=true` neutralizes the threat for most Java versions. Spigot and many other services have already inserted the flag into the games they make available to users.

To add the flag users should go to their launcher, open the installations tab, select the installation in use and click "..." > "Edit" > "MORE OPTIONS", and paste `-Dlog4j2.formatMsgNoLookups=true` at the end of the JVM flags.

For the time being, people should pay close attention to this vulnerability and its potential to trigger high-impact attacks against a wide variety of apps and services. For *Minecraft* users, that means steering clear of unknown servers or untrustworthy users. For users of open source software, it means checking to see if it relies on Log4j or Log4j2 for logging. This is a breaking story. Updates will follow if more information becomes available.