advance

The Vulnerability That Has The Security Community in Meltdown - Log4Shell explained

INTRODUCTION

Log4Shell, or Logjam, is the name security researchers have given the newly disclosed vulnerability that threw security experts into crisis mode in early December. The name comes from the software package which has the vulnerability, which is called Log4j and is a part of the very common programming framework, Java.

In short, it is an extremely easy-to-exploit vulnerability that affects millions, if not billions, of devices, systems and programs worldwide, making it a very serious concern in the world of cybersecurity.

WHAT IS IT?

The vulnerability exists within a standard way for systems to record information about what they are processing, known as logging. A computer may log information entered by users, such as usernames or clicks, or system data, such as error messages and error times. These logs can then be used later to troubleshoot issues, or better understand how the computer is working.

The Log4Shell vulnerability exists because when a specific, malicious combination of text is logged, the logging computer sees the text as a command to be executed rather than information to be entered into the log. The malicious command tells the computer to connect to a separate, external computer and download a program. If the attacker has written the text correctly, this second computer will be one they control, and the program it downloads will be anything the attacker chooses, likely something malicious.

For example, an attacker could pretend to “log in” to Facebook. Instead of a username, they insert a command they have written that exploits this vulnerability. The login fails, of course, but in the background, Facebook logs the failed attempt along with the “username”. The Facebook server sees the username as a command, connects to the external computer where the attacker has left a virus, and suddenly a virus has entered Facebook’s network[1].

The issue was first discovered in the game Minecraft, where users were able to enter the malicious command in the chat. This would cause the game’s servers to connect to an external computer and download a program which crashed the game for everybody connected. This has since evolved and has now been observed installing ransomware on Minecraft servers[2].

In another example, one security researcher found Apple’s network to be vulnerable, and was able to prove how easy it was to exploit by simply renaming his iPhone with the malicious text. Once the iPhone was backed up by Apple overnight, the backup servers processed the iPhone name, recognised it as a command, and connected to the external server set up by the researcher[3].

[1] Please note, there is no indication that Facebook is vulnerable to this issue, we have simply used them as an example to demonstrate one way this vulnerability could be exploited.
[2]https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/
[3]https://twitter.com/chvancooten/status/1469340927923826691

WHY ARE RESEARCHERS SO WORRIED?

The cybersecurity industry has an unfortunate reputation of sounding doomsday alarms too early. But while Log4Shell certainly won't signal the end of the digital world, it's certainly a very concerning issue.

Jen Easterly, who is director of the US Cybersecurity and Infrastructure Security Agency (CISA) and is known for her level-headed approach, characterised Log4Shell as "*one of the most serious I've seen in my entire career, if not the most serious*"[4] . So why is the cybersecurity community especially worried about this particular vulnerability? Here are three reasons:

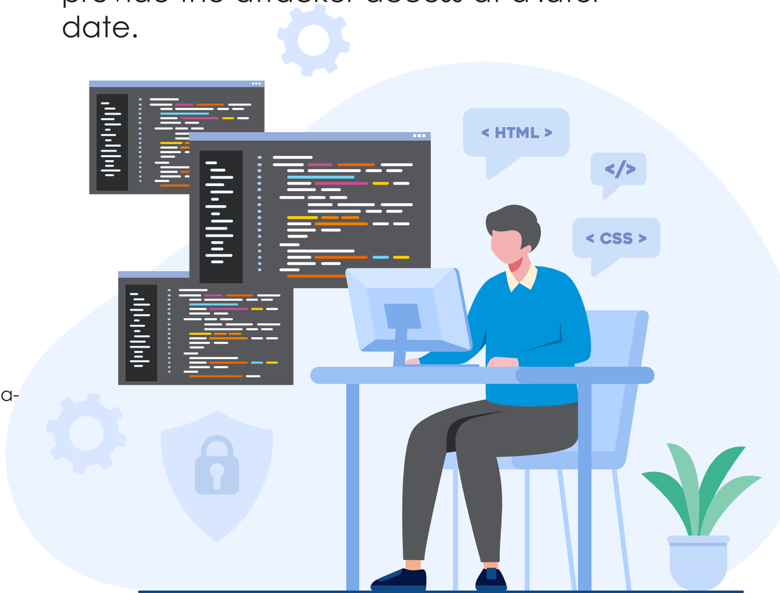
Ease of use – Most serious vulnerabilities in modern software are quite hard to exploit. They often require specialist knowledge, and the chaining together of multiple security flaws before an attacker gets to run their own malicious programs in a secure environment.

Log4Shell is the complete opposite, with many security experts describing it as trivial for an attacker to exploit and gain full control of a target computer. The initial malicious text is only a few words long and is publicly available. All a would-be attacker needs to do is place their malicious program on the internet and insert the location into the text, and their target will download and run it.

Widespread exposure – The program with the vulnerability, log4j, is a common element of a very popular programming language. Programmers don't reinvent the wheel each time they build a new program; instead, they use publicly available libraries to achieve common requirements, such as logging. Log4j was downloaded more than 80 million times[5] in the last four months alone, and the CISA estimates the number of vulnerable devices to be in the hundreds of millions[6].

Threat actor activity – Due to the first two reasons, cyber threat actors have been extremely quick to take advantage of the Log4Shell vulnerability. Within hours of its public disclosure, specialist programs had been created to scan the internet, hunting for computers vulnerable to Log4Shell. Internet and security infrastructure providers are already reporting millions of attempts to use the vulnerability, and it's estimated that more than 50% of Australian businesses have already been probed by cybercriminals looking for a way in[7].

In less than one week of Log4Shell being publicly disclosed, there have already been many reports of it being used to deploy Ransomware and malicious crypto miners. However, these incidents that have been detected and reported are just the tip of the iceberg. The area of most concern is the unknown number of times Log4Shell has been used to deploy more subtle, or time-bomb style malicious programs that will cause future damage or provide the attacker access at a later date.



[4] https://www.cyberscoop.com/log4j-cisa-easterly-most-serious/
[5] https://www.bbc.com/news/technology-59669297
[6] https://www.cyberscoop.com/log4j-cisa-easterly-most-serious/
[7] https://blog.checkpoint.com/2021/12/13/the-numbers-behind-a-cyber-pandemic-detailed-dive/

IT'S NOT ALL DOOM AND GLOOM

Despite the concerning aspects of the Log4Shell vulnerability, there are several positive points to the situation.

The vulnerability was first discovered by the security team of Chinese technology giant Alibaba. It was privately disclosed to the developers of log4j on the 24th of November, two weeks before it went public. This gave the developers time to document a fix, as well as create a software patch, both of which are available to anyone.

In addition to the patch, there are other ways to prevent this vulnerability being exploited.

Vendors such as Cloudflare, who provide secure internet hosting infrastructure, and Check Point, who provide intrusion prevention technologies, have been able to update their solutions to identify and block attempts to exploit Log4Shell.

At time of writing these companies are reporting blocking millions of attempted exploits per day[8, 9], despite not owning the computers that need patching.

This is a great demonstration of the defensive layers concept that has become popular in modern security, with vulnerable applications being protected by other security solutions until the patch can be applied.

[8] https://www.bbc.com/news/technology-59669297
[9] https://blog.checkpoint.com/2021/12/13/the-numbers-behind-a-cyber-pandemic-detailed-dive/

WHAT WE ARE DOING ABOUT IT

At Advance, we offer a series of monitoring services around cyber-security. These services are designed to monitor not only the health of your network but any vulnerabilities or threats which may be present in your on-premise or cloud hosted applications.

Communication and education are paramount for protecting clients in all aspects of their network, applications and environment in general.

Advance's key philosophy is providing the right information at the right time for your organisation and its staff. While we monitor and protect your environment we also ensure that any new threats, issues or vulnerabilities are communication to you so you're aware and able to act in time.

- Monitoring against all known threats and vulnerabilities in hardware and applications
- Easy to manage by:
    - Actively Identifying how you are at risk
    - Prioritising the level of risk or threat
    - Take action to remove the threat or correct the vulnerability
- All this is done in a monthly service agreement for your peace of mind

CONCLUSION

Unfortunately, in today's world of complex and inherited computer code, these vulnerabilities will continue to be discovered and exploited. They cannot be avoided entirely, but they can be planned for.

An IT partner with a strong security pedigree, a solid response plan, a known mapping of software and its supporting vendor, and a robust emergency patching process can be an invaluable asset to a business to help them respond to, contain, and mitigate the impact of cybersecurity issues like this on their day-to-day operations.

Contact Info

☎ +61 8 8238 6500

✉ sales@advance.net.au

🌐 www.advance.net.au

Please note, this document was published in December 2021. Log4Shell continues to be an evolving issue, we expect to publish future updates.