CLCT

WILLIAM & MARY LAW SCHOOL

Cybersecurity and Information Security Newsletter

Issue 14 | January 14, 2022

Table of Contents

- The open source software community and government agencies rush to contain a novel Log4j 2 vulnerability
- The U.S. Cyberspace Solarium Commission releases white paper focusing on countering disinformation

Happy New Year! Daniel Shin, research scientist with the Commonwealth Cyber Initiative (CCI) Coastal Virginia region, wants to hear from you! Submit any cybersecurity and information security news items or request related topics, via e-mail to dshin01@wm.edu.

This newsletter supports the mission of CCI. To learn more about CCI, including upcoming events, funded research, and news, please visit cyberinitiative.org.

The open source software community and government agencies rush to contain a novel Log4j 2 vulnerability

On November 24, 2021, Chen Zhaojun (Chen) of the Alibaba Cloud Security Team alerted the Apache Software Foundation (ASF) about a Log4j 2 vulnerability that could allow knowledgeable threat actors to hijack computer systems running Log4j 2. *Inside the Race to Fix a Potentially Disastrous Software Flaw (Bloomberg)*, available here.

Log4j 2 is a programming framework (prepackaged set of code that is used by programmers) widely used to record certain events from targeted systems. Log4j 2 is based on its predecessor, Log4j 1.X, and offers certain enhanced features for programmers. On August 5, 2015, Log4j 2 became the primary version utilized in software development as all other previous versions became obsolete. Currently, this framework is widely used in web-based software applications.

To explain what Log4j 2 does, think about Event Data Recorders (EDRs) (commonly known as a "black box"), which are found on automobiles and airplanes. Vehicle manufacturers install third-party EDRs to delegate the task of recording data generated by the vehicle (for instance, speed and location). In the same way, program developers delegate program-logging features to third-party programming frameworks, such as Log4j 2. Log4j 2 is considered one of the most commonly used framework. *Log4shell by the numbers- Why did CVE-2021-44228 set the Internet on Fire?*, available here. In fact, it is even used by the Ingenuity helicopter on the Mars rover! *Did you know that Ingenuity, the Mars 2020 Helicopter mission, is powered by Apache Log4j? (Twitter)*, original page deleted but the archived page available here.

The Log4j 2 vulnerability identified by Chen could allow a threat actor to send a carefully crafted message to a server running a susceptible Log4j 2 component to eventually install and run other programs without authorization. In essence, this vulnerability bypasses other system security mechanisms and allows threat actors to control vulnerable systems.

After verifying Chen's claims, the ASF began creating a software fix to address the framework's exposure. In the meantime, on December 8, 2021, Chen contacted the ASF again, this time alerting them that the Log4j 2 vulnerability was revealed on a Chinese blogging platform, and "[s]ome WeChat security chat groups are already discussing the details of the vulnerability, and some security researchers already have the vulnerability." *Inside the Race to Fix a Potentially Disastrous Software Flaw (Bloomberg)*, *supra*. Chen promised not to disclose the vulnerability until the ASF could publicly release an appropriate fix. Chen impressed on the ASF the need to "[p]lease hurry up." *Id.*

Soon thereafter, the ASF published multiple software updates to resolve the vulnerability, although security researchers have identified issues with previously published fixes. *Log4j Zero-Day Vulnerability Response (Center for Internet Security)*, available here. The Center for Internet Security expects a continuous stream of fixes before this vulnerability is completely mitigated. *Id.*

According to Matthew Prince, co-founder and CEO of Cloudflare (a U.S.-based web infrastructure and security company), the earliest known instance of this vulnerability being exploited was on December 1, 2021. *Matthew Prince's Tweet (Twitter)*, available here. Similarly, a proof of concept for exploiting this vulnerability was posted as early as December

9, 2021. *CVE-2021-44228(Apache Log4j Remote Code Execution)*, original page deleted but the archived page available here.

In response to the Log4j 2 vulnerability, the Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security published its Log4j Scanner that allows system administrators to determine whether their systems are potentially affected by the vulnerability. *Log4j Scanner (GitHub)*, available here. Also, the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce has been continuously tracking the vulnerability via its National Vulnerability Database. *CVE-2021-44228*, available here. Finally, on January 4, 2022, the Federal Trade Commission (FTC) announced its intentions "to use its full legal authority to pursue companies that fail to take reasonable steps to protect consumer data from exposure as a result of Log4j, or similar known vulnerabilities." *FTC warns companies to remediate Log4j security vulnerability*, available here. Under the Federal Commission Act and the Gramm Leach Bliley Act, companies have legal obligations to take reasonable steps to mitigate known software vulnerabilities that can cause "loss or breach of personal information, financial loss, and other irreversible harms." *Id.* In the past, the FTC has pursued companies, such as Equifax, for failing to reasonably secure sensitive consumer personal information. *Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach*, available here.

While CISA and other companies have released tools that check for Log4j 2 vulnerabilities in systems, these tools are not easy to use for non-technical users. Because Log4j 2 is akin to an internal component of a complex machine, this vulnerability cannot be manually patched by consumers who may be using programs that use the vulnerable Log4j 2 code. As such, consumers should patch any software updates from developers because those updates may fix any issues stemming from the Log4j 2 vulnerability. Thus, it is up to software developers to determine whether their published programs are vulnerable to this exploit, and patch this vulnerability promptly to prevent users' systems from being compromised by it.

Although Chen is credited with, and widely praised for, discreetly revealing the vulnerability to the ASF, China's Cyber Security Administration of the Ministry of Industry and Information Technology (MIIT) penalized Chen's employer, Alibaba Cloud Computing (a China-based cloud computing service company), for failing to promptly report it to Chinese government authorities. *独家丨阿里云被暂停工信部网络安全威胁信息共享平台合作单位 [Exclusive 丨 Alibaba Cloud is suspended from the Ministry of Industry and Information Technology's cybersecurity threat information sharing platform cooperation unit]*, available here. It is understood that under Article 2 of the Provision on Security Loopholes of Network Products (a cybersecurity governmental regulation of China), network product providers are obligated to report vulnerability information to the MIIT's Cyber Security Threat and Vulnerability Information sharing platform within two days of discovery. *网络产品安全漏洞管理规定 (Regulations on the Management of Security Vulnerabilities in Network Products)*, available here. Although Chen reportedly knew of the Log4j 2 vulnerability as early as November 24, allegedly, MIIT was first notified of the vulnerability by an unnamed network security professional organization on December 9, 2021. *关于阿帕奇 Log4j2 组件重大安全漏洞的网络安全风险提示（中华人民共和国工业和信息化部）[Cybersecurity risk tips on major security vulnerabilities in Apache Log4j2 components (Ministry of Industry and Information Technology*

of the People's Republic of China)], available here. Consequently, Alibaba Cloud Computing's cybersecurity partnership with the MITT was suspended for six months.

Analysis

Despite providing useful event-logging features to programmers, Log4j 2 has historically suffered from vulnerabilities that allowed threat actors to execute unauthorized code on targeted servers. The common cause of previous vulnerabilities involved the exploitation of Log4j 2's feature of accepting external data sources for logging purposes. *Another Apache Log4j Vulnerability Is Actively Exploited in the Wild (CVE-2021-44228) (Updated Dec. 28) (Palo Alto Networks – Unit 42)*, available here. By carefully crafting and feeding a malicious data stream to a server using Log4j 2, security analysts were able to induce Log4j 2 to behave in unexpected ways that could be exploited for infiltration purposes. *See, e.g., CVE-2017-5645 (NIST)*, available here; *CVE-2019-17571 (NIST)*, available here.

Unlike other software vulnerabilities, Log4j 2 vulnerability is unique due to the widespread use of this software component. Researchers have been able to identify various web services, including certain versions of Minecraft servers (a popular server used to host the game Minecraft), being vulnerable to this exploit. *See Log4jAttackSurface (GitHub)*, available here. The widespread implication of this vulnerability has led some to label this exploit as a "cluster bomb of zero days." *CVE-2021-44228 - Log4j - MINECRAFT VULNERABLE! (and SO MUCH MORE) (YouTube)*, available here. Fortunately, both CISA and NIST have provided up-to-date resources to document this vulnerability for the cybersecurity community. Furthermore, the FTC's announcement on Log4j 2 remediation requirements serves as an effective measure to encourage companies to investigate and mitigate this vulnerability. Also, the ASF has been active in providing Log4j 2 updates to mitigate the vulnerability.

Finally, Chen deserves much credit for withholding information except from those who may have the best ability to resolve this issue *for everyone*. Public disclosure of novel cybersecurity vulnerabilities without appropriate remedies in place risks creating more opportunities for threat actors exploiting them before systems could develop or apply remedial solutions. Chen's action demonstrates the goodwill and global cooperative nature of security professionals across national boundaries. It is likely that Chen acted on his own volition to handle his vulnerability discovery for the sake of the global open source community. As a result, the potential damage resulting from this vulnerability was highly mitigated, even though Chen's employer was reprimanded for violating China's cybersecurity vulnerability disclosure regulation.

*This newsletter would especially like to recognize Zeyi Yang of Protocol, an online publication, for the thorough references to Chinese news sources and official legal references in his article. *Beijing punishes Alibaba for not reporting Log4j loophole fast enough*, *supra*.

The U.S. Cyberspace Solarium Commission releases white paper focusing on countering disinformation

On December 16, 2021, the U.S. Cyberspace Solarium Commission (CSC) released the white paper *Countering Disinformation in the United States* that offers policy recommendations to counter disinformation and promote a resilient information system. *Cyberspace Solarium Commission White Paper #6: Countering Disinformation in the United States*, available here.

The CSC was established by the National Defense Authorization Act for Fiscal Year 2019 with the aim of "develop[ing] a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences." *About*, available here. The CSC is composed of ten Commissioners, including four U.S. legislators and five "nationally recognized experts from outside of government." *Id.* It has published various policy recommendations in the area of national cybersecurity.

CSC's disinformation white paper focuses on the national threat of foreign government-led disinformation campaigns targeting the U.S. public sphere. The CSC observed that foreign adversaries have continued spreading disinformation beyond the 2020 President Election and into the COVID-19 pandemic. *Cyberspace Solarium Commission White Paper #6: Countering Disinformation in the United States*, *supra* at 4 ("[foreign] adversaries' disinformation campaigns focused on the pandemic illustrate that disinformation activities can reach far beyond the political and electoral contexts . . . ."). Both members of Congress and some in the executive branch have reached out to the CSC to explore the topic of disinformation and provide relevant policy recommendations.

The white paper focuses on increasing visibility of disinformation within the U.S. information ecosystem and encouraging the federal government's partnership with relevant stakeholders to counter disinformation campaigns by foreign adversaries without direct government involvement.

The white paper offers seven recommendations to Congress, which include:

1. Establishing a Civic Education Task Force at the Department of Education (DOE) that aims to enable greater access to civic education resources and raise public awareness about foreign disinformation;
2. Providing material support to nongovernmental disinformation researchers;
3. Funding grants to nonprofit centers that focus on identifying, exposing, and explaining malign foreign influence campaigns to the public;
4. Allowing the Department of Homeland Security to actively monitor foreign disinformation campaigns;
5. Creating grant programs that assist state and local governments with the personnel and resources necessary to identify foreign disinformation campaigns and incorporate countermeasures into public communications strategies;
6. Reforming the Foreign Agents Registration Act and directing the Federal Communications Commission to introduce new regulations that improve media ownership transparency; and
7. Granting to a not yet specified federal entity the authority to publish and enforce transparency guidelines for social media platforms.

Despite the national threat of disinformation, the white paper emphasizes that the role of the federal government to counter disinformation should be narrow and purposeful. This is because the appearance of governmental influence on the domestic information space may suggest an inappropriate propaganda campaign. Furthermore, it notes that education, which plays a critical role in building a resilient information ecosystem, is largely a policy area led by the states and not the federal government. As such, the seven recommendations avoid federal action to confront directly the threat of foreign-led disinformation campaigns. Instead, the CSC focuses on redirecting federal resources to fund non-federal key stakeholders.

Analysis

Investing in information literacy provides a critical barrier against disinformation campaigns and promotes a resilient republic. Recognizing this need, CSC's first recommendation calls for establishing a Civic Education Task Force at DOE tasked with making publicly available civic education, and digital and media literacy courses for the broader adult population. *Cyberspace Solarium Commission White Paper #6: Countering Disinformation in the United States*, supra at 18 (emphasis added), *supra*.

On November 29, 2021, the Government Communications Headquarters of the U.K. (GCHQ) published a paper titled *Ethics of AI: Pioneering a New National Security*, where it explores utilizing AI technologies to support law enforcement operations and maintain national interests. *Ethics of AI: Pioneering a New National Security*, available here. The paper suggests using AI technologies to fact-check and detect deepfake media (realistic but false media that is generated using deep learning techniques) propagated by foreign governments.

In addition to the CSC's disinformation policy recommendations, the federal government's investment in practical AI technologies may provide automated means to detect and label disinformation in the U.S. One of the key challenges of disinformation campaigns is the prevalence of disinformation on information ecosystems. Similar to how GCHQ plans to use AI technologies to detect false AI-generated media, the federal government should encourage the development of feasible automated technologies (e.g., machine learning) that can scan and label disinformation in a haystack of other information.

Finally, 18 U.S.C. § 2071 allows the U.S. government to pursue individuals for willfully and unlawfully mutilating or falsifying any documents published by the federal government, regardless of where those documents were located. *18 U.S.C. § 2071*, available here; *See U.S. v. De Groat*, 30 F. 764 (E.D.Mich. 1887), available here. Section 2071 has not been commonly used for prosecution purposes, but it may provide a mechanism to prosecute those who intentionally alter government documents—a broad term capturing several means of communication—to facilitate disinformation campaigns.

Countering disinformation requires a multi-prong approach, and the CSC's recommendation offers a much-needed blueprint for the federal government to tackle this issue and promote a healthy information ecosystem. Policymakers and key stakeholders should continue monitoring the disinformation landscape and consider various proactive approaches to mitigate this ongoing issue.