Review of the December 2021 Log4j Event

Publication: July 11, 2022
Cyber Safety Review Board

Table of Contents

Table of Contents ..... *i*

Message from the Chair and Deputy Chair ..... *ii*

Executive Summary ..... *iv*

Review Methodology ..... *vii*

Section 1 – Factual Information *1*

1.1 Genesis of the Vulnerability 1

1.2 Discovery and Disclosure 1

1.3 Exploitation 3

1.4 Response 5

Section 2 – Findings and Conclusions *10*

2.1 Summary of Findings 10

2.2 Contributing Factors of the Vulnerability 11

2.3 Enterprise Risk Management 12

2.4 Ecosystem Risk Management 13

2.5 Impact on Business Operations 16

Section 3 – Recommendations *18*

Address Continued Risks of Log4j 18

Drive Existing Best Practices for Security Hygiene 20

Build A Better Software Ecosystem 23

Investments in the Future 26

Appendix A: CSRB Principles *29*

Appendix B: Summary of CSRB Interviews and Requests for Information *30*

Appendix C: Precursors to CVE-2021-44228 Discovery *33*

Appendix D: Communications Overload *35*

Appendix E: Observations on the Open Source Software Ecosystem *38*

Appendix F: Practices Contributing to Event Response and Management *39*

Appendix G: Cyber Safety Review Board Members *41*

Appendix H: Acronyms *42*

MESSAGE FROM THE CHAIR AND DEPUTY CHAIR

We write this report at a transformational moment for the digital ecosystem. The infrastructure on which we rely daily has become deeply interconnected through the use of shared communications, software, and hardware, making it susceptible to vulnerabilities on a global scale. While the computing industry is maturing, our ability to handle risk and incidents in our digital ecosystems is not keeping pace. To address this gap, and to begin driving necessary systemic improvements, President Biden directed the establishment of the Cyber Safety Review Board (CSRB, or the Board) to review significant cyber incidents and provide "advice, information, or recommendations for improving cybersecurity and incident response practices and policy."[1]

We were honored to take the helm of the CSRB at this critical juncture. To advance the overall security and resiliency of our digital ecosystem, we applaud the application of this highly effective lessons-learned model from other industries. With the discovery of major software vulnerabilities and gaps in our capabilities to effectively mitigate them, we believe this effort will help drive improvements in our overall cyber resiliency.

The Board's first charge was to review the events surrounding the December 2021 disclosure of the Log4j vulnerability. Log4j is a piece of open source software that developers have integrated into millions of systems. A vulnerability in such a pervasive and ubiquitous piece of software has the ability to impact companies and organizations (including governments) all over the world. As such, the Log4j event drives home the urgency with which we must move to a culture of shared responsibility around managing cyber threats. The scope of this report, and to whom we are directing the recommendations, reflect this observation.

The review of the Log4j event presented the Board with several challenges. First, unlike comparable studies of incidents in other sectors (such as transportation), we had no crash site or damaged vehicle to inspect, no stress tests to perform on failed equipment, and no wiring diagrams to review. Instead, we reviewed practices used to create and adopt technology, ecosystems, and processes. We relied on subject matter experts in open source software, its development, deployment, and maintenance. In our discussions, we observed enthusiasm for tackling these issues, and also the community's desire to have a more fulsome picture of where vulnerabilities lie, which of them are exploitable, and the effectiveness of remediations.

Second, the Log4j event is not over. Log4j remains deeply embedded in systems, and even within the short period available for our review, community stakeholders have identified new compromises, new threat actors, and new learnings. We must remain vigilant against the risks associated with this vulnerability, and apply the best practices described in this review.

Third, there is a real need to drive widespread development and adoption of capabilities, tooling, and automated frameworks that support developers with the daunting task of building secure software. Just as the software industry has enabled the democratization of software programming—the ability for anyone to generate software with little or no formal training—we must also democratize security by baking security by default into the platforms used to generate, build, deploy, and manage software at scale.

An open question at the start of our work was the extent to which we would receive voluntary cooperation from industry stakeholders. We have been heartened by the outpouring of offers from industry to support the Board's review through insights and data. We have spoken with and received data from a substantial number of companies and security experts. We believe industry has come to understand that the Board is not an enforcement or regulatory body and is not focused on assigning blame. The Board instead looks forward, making recommendations to better secure the community for the future. We give thanks to the many companies and individual experts that offered their support for the Board's comprehensive review.

As this was the inaugural review for the Board, we humbly sought to create the foundations for a sustainable and impactful body that would drive systemic improvements. At our first meeting on February 25, 2022, we agreed to a set of principles, both for this review and beyond, that embody this Board's commitment to public service, transparency and trust, and objective, forward-looking reviews. See Appendix A for the principles that guided the Board's work throughout our review.

---

[1] Executive Order (EO) 14028, "*Improving the Nation's Cybersecurity*," May 12, 2021, https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

We are grateful to Secretary of Homeland Security Alejandro Mayorkas for launching this Board and providing his strategic vision, and to Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly for commissioning our initial review of the Log4j vulnerability and offering CISA's resources and support to ensure the Board could conduct its independent work.

Finally, we express our appreciation for our colleagues on the Board and the talented and dedicated CSRB project team. We are deeply grateful to you for coming on this journey. Together we have launched a new fixture of the cybersecurity ecosystem, and set the stage for many incident reviews to come.

Robert Silvers
Chair
Cyber Safety Review Board

Heather Adkins
Deputy Chair
Cyber Safety Review Board

EXECUTIVE SUMMARY

The scale and efficiency of our global technology infrastructure are made possible through the standardization of key building blocks. These reusable building blocks, while useful for creating software at scale, also create dependencies and risks that are often not understood until they manifest as a security issue. For example, a vulnerability in a software building block that is integrated into numerous other software packages means that every organization that uses those packages is at risk. It also means that system owners may not know where vulnerable software lives within their environments. When such a vulnerability is also easy for a threat actor to exploit to obtain broad control over a compromised system, it can create a once-in-a-generation security event. This is what happened with the Log4j vulnerability that came to public attention in December 2021.

Apache Log4j is an open source Java-based logging framework that collects and manages information about system activity. Log4j is simple to use, free to download, and effective in its intended function, making it popular among Java developers, who have embedded it into thousands of other software packages. Log4j version 2, the primary topic of this report, was initially released in 2012. In 2013, prior to the general availability release in 2014 and through a standard process, the Log4j team accepted a community-submitted feature intended to ease data storage and retrieval called "JNDI [Java Naming and Directory Interface™] Lookup plugin support." This addition was subsequently integrated into thousands of applications in which Log4j is used.

On November 24, 2021, a security engineer from the Alibaba Cloud Security team, within the People's Republic of China (PRC), reported a vulnerability in the JNDI feature to the Apache Software Foundation (ASF), a non-profit corporation that provides support for the Log4j project.[2, 3] While ASF was working to understand the issue and devise a fix, another party disclosed the vulnerability before ASF made an upgrade available to the general public. Such a disclosure of a significant vulnerability in any widely used piece of software immediately triggers a race between defense and offense: a race to apply upgrades before threat actors exploit vulnerable systems. The Log4j vulnerability was no exception.

Defenders faced a particularly challenging situation; the vulnerability impacted virtually every networked organization and the severity of the threat required fast action. The fact that there is no comprehensive "customer list" for Log4j, or even a list of where it is integrated as a sub-system, hindered defender progress. Enterprises and vendors scrambled to discover where they used Log4j. The pace, pressure, and publicity compounded the defensive challenges: security researchers quickly found additional vulnerabilities in Log4j, contributing to confusion and "patching fatigue"; defenders struggled to distinguish vulnerability scanning by bona fide researchers from threat actors; and responders found it difficult to find authoritative sources of information on how to address the issues. This culminated in one of the most intensive cybersecurity community responses in history.

Responders, spanning the public and private sectors, the open source community, and researchers globally, collaborated and communicated in a dedicated fashion, working through weekends and the December holidays. The Board noted high levels of cooperation, extensive use of social media for rapid sharing of mitigation advice, innovative response actions from the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), and the creation of new shared community resources.

Generally, the Cyber Safety Review Board (CSRB, or the Board) found that organizations that responded most effectively to the Log4j event understood their use of Log4j and had technical resources and mature processes to manage assets, assess risk, and mobilize their organization and key partners to action. Most modern security frameworks call out these capabilities as best practices. However, few organizations were able to execute this kind of response, or the speed required during this incident, causing delays in both their assessment of the risk and in their management of it. When ASF made upgrades for Log4j available, deploying them was itself a risk decision, forcing a tradeoff between possible operational disruption and timeliness, completeness, and compensating controls.

Organizations spent significant resources as they struggled with this problem. For example, one federal cabinet department reported dedicating 33,000 hours to Log4j vulnerability response to protect the department's own

[2] Apache Software Foundation (ASF). Response to Board request for information. April 25, 2022.
[3] Leadership and Security team; Apache Software Foundation (ASF). Board Meeting.

networks. These costs, often sustained over many weeks and months, delayed other mission-critical work, including the response to other vulnerabilities.

For the long term, we will continue to see the tension between our collective need for crisis-driven risk management and the foundational investments that would support more rapid response for future incidents. Perhaps most significantly, the force exerted on the urgent response and the challenges in managing risk also contributed to professional "burnout" among defenders that may, compounded with the generally intense pace of many cybersecurity jobs, have a long-term impact on the availability of cybersecurity talent.

At the time of writing, the Board is not aware of any significant Log4j-based attacks on critical infrastructure systems. Somewhat surprisingly, the Board also found that to date, generally speaking, exploitation of Log4j occurred at lower levels than many experts predicted, given the severity of the vulnerability. It has been difficult to arrive at this conclusion. While cybersecurity vendors were able to provide some anecdotal evidence of exploitation, no authoritative source exists to understand exploitation trends across geographies, industries, or ecosystems. Many organizations do not even collect information on specific Log4j exploitation, and reporting is still largely voluntary.

Most importantly, however, the Log4j event is not over. The Board assesses that Log4j is an "endemic vulnerability" and that vulnerable instances of Log4j will remain in systems for many years to come, perhaps a decade or longer. Significant risk remains.

The Log4j event illustrates how counterintuitive cybersecurity defense can be, for both individual enterprises and for the ecosystem as a whole. Many things went "right": ASF had a well-established software development lifecycle with clear roles for vetting, testing, and approving new code; security researchers followed generally accepted steps of coordinated disclosure; ASF recognized the criticality of the problem and software developers made upgrades available; vendors and governments rapidly produced guidance, tools, and threat information, often in novel and beneficial ways; and the whole ecosystem rallied behind a collective sense of urgency. Yet organizations still struggled to respond to the event, and the hard work of upgrading vulnerable software is far from complete across many organizations.

The event also called attention to security risks unique to the thinly-resourced, volunteer-based open source community. This community is not adequately resourced to ensure that code is developed pursuant to industry-recognized secure coding practices and audited by experts. To reduce recurrence of the introduction of vulnerabilities like Log4j, it is essential that public and private sector stakeholders create centralized resourcing and security assistance structures that can support the open source community going forward.

In the course of the review, the Board also evaluated press reports suggesting that Alibaba violated PRC law and was subsequently sanctioned by the PRC government. The Board could not identify any publicly available official explanation, and while the PRC government provided a statement to the Board about the Log4j event on behalf of the Ministry of Industry and Information Technology (MIIT), it did not provide an answer to the Board's request for information about any sanction imposed on Alibaba. This line of inquiry raised Board concerns around the mandatory vulnerability disclosure laws in the PRC and whether their enforcement may afford the PRC government early access to serious, exploitable vulnerabilities before they are patched. The Board raised similar concerns about whether these laws and reports of the PRC's alleged decision to sanction Alibaba for responsibly reporting a vulnerability to ASF will create a chilling effect that deters researchers from using coordinated vulnerability disclosure best practices.

The CSRB's mandate was to review the events surrounding this consequential vulnerability, report on lessons learned, and make independent, strategic, and actionable recommendations to the Secretary of Homeland Security. Using data collected from extensive interviews and requests for information, we have framed our report in three sections: Factual Information (facts describing what happened); Findings and Conclusions (an analysis of the facts); and Recommendations. The Recommendations are broken into four categories.

Address Continued Risks of Log4j: continued vigilance in addressing Log4j vulnerabilities for the long term.

1. Organizations should be prepared to address Log4j vulnerabilities for years to come.
2. Organizations should continue to report (and escalate) observations of Log4j exploitation.

3. CISA should expand its capability to develop, coordinate, and publish authoritative cyber risk information.
4. Federal and state regulators should drive implementation of CISA guidance through their own regulatory authorities.

Drive Existing Best Practices for Security Hygiene: adopt industry-accepted practices and standards for vulnerability management and security hygiene.

5. Organizations should invest in capabilities to identify vulnerable systems.
6. Develop the capacity to maintain an accurate information technology (IT) asset and application inventory.
7. Organizations should have a documented vulnerability response program.
8. Organizations should have a documented vulnerability disclosure and handling process.
9. Software developers and maintainers should implement secure software practices.

Build a Better Software Ecosystem: drive a transformation in the software ecosystem to move to a proactive model of vulnerability management.

10. Open source software developers should participate in community-based security initiatives.
11. Invest in training software developers in secure software development.
12. Improve Software Bill of Materials (SBOM) tooling and adoptability.
13. Increase investments in open source software security.
14. Pilot open source software maintenance support for critical services.

Investments in the Future: pursue cultural and technological shifts necessary to solve for the nation's digital security for the long run.

15. Explore a baseline requirement for software transparency for federal government vendors.
16. Examine the efficacy of a Cyber Safety Reporting System (CSRS).
17. Explore the feasibility of establishing a Software Security Risk Assessment Center of Excellence (SSRACE).
18. Study the incentive structures required to build secure software.
19. Establish a government-coordinated working group to improve identification of software with known vulnerabilities.

REVIEW METHODOLOGY

The Board engaged with nearly 80 organizations and individuals representing software developers, end users, security professionals, and companies. These engagements included a mixture of interviews and requests for information. The Board is grateful for the voluntary participation of these parties that came forward and provided timely responses. Their efforts helped the Board collect the observable timeline of events, corroborate facts, and understand the complex dimensions of the Log4j event.

The Board sought to speak to representatives from a wide variety of viewpoints, to capture the nuances of how different attack surfaces are designed and defended. We acknowledge that in the 90-day review period, we were not able to reach all sectors and that some, such as medical devices, Internet-of-Things (IoT), and home networking equipment, may have alternative experiences not captured in this report. Similarly, we recognize that organizations outside of the United States may have experienced the Log4j event in unique ways. Nonetheless, we believe the Board's findings and recommendations apply to a wide variety of global organizations, given the interconnected nature of the stakeholders from whom we did hear. See Appendix B for a list of participating organizations and individuals.

This report is divided into three major sections:

> **Section 1: Factual Information,** provides a timeline of the Log4j vulnerability's progression, as well as the key facts of what happened during the event;
>
> **Section 2: Findings and Conclusions,** presents the Board's key findings with respect to the Log4j event; and
>
> **Section 3: Recommendations,** outlines action items the Board recommends for a variety of stakeholders in the private and public sector.

Taken together, these sections tell the story of Log4j and the key stakeholders impacted and provide both industry and government alike with a set of lessons learned that can be applied to prevent or respond more effectively to future incidents.

A Note on Terminology

To simplify the readability of this report, references to Apache Log4j (the original Log4j package) and Apache Log4j 2 (version 2) will be shorted to Log4j. The primary vulnerability at the center of the event and this review (CVE-2021-44228) will be known as the Log4j vulnerability, unless further specificity is useful.

SECTION 1 – FACTUAL INFORMATION

Log4j is an open source Java-based logging framework that collects and manages information about system activity. Since the software's inception in 1999, it has become a popular building block for the ecosystem, with developers incorporating Log4j into thousands of other software packages globally. A group of volunteers maintain Log4j under the Apache Software Foundation's (ASF) Apache Logging Services™ Project.[4]

1.1 GENESIS OF THE VULNERABILITY

In July 2013, a member of the open source community requested the addition of a new data storage and retrieval mechanism ("Java Naming and Directory Interface™ [JNDI] Lookup plugin support") to the Log4j project.[5] The requester provided a software patch that implemented the requested functionality, which the Log4j project team reviewed and committed on July 18, 2013 for release in version 2.0-beta9.[6] The vulnerability was due to the following technical reason:

JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP [Lightweight Directory Access Protocol] and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.[7]

This means an attacker who gains access to logging messages could inject fraudulent messages that enable arbitrary code execution and exploitation of a vulnerable system.[8]

See Appendix C for additional information on Log4j development and deployment and JNDI-related risks.

1.2 DISCOVERY AND DISCLOSURE

On November 24, 2021, a security engineer from the Alibaba[9] Cloud Security team in the People's Republic of China (PRC) reported the discovery of a vulnerability in Log4j to ASF via email.[10] The engineer included pertinent information about the vulnerability, including a description of the issue, a pointer to the vulnerable code, a proof of concept, and screenshots.[11]

Once ASF became aware of the vulnerability, its intent was to develop a patch as quickly as possible, in accordance with its policy. ASF also assessed that, due to the widespread use of Log4j, placing an embargo[12] on the vulnerability would be impractical.[13] ASF began reviewing code for the fix as early as November 29,

---

[4] Apache Software Foundation (ASF), "Apache Log4j 2," February 23, 2022, https://logging.apache.org/log4j/2.x/
[5] Apache Software Foundation (ASF), "Log4j 2 Issues: LOG4J 2-313, JNDI Lookup plugin support," July 17, 2013, https://issues.apache.org/jira/browse/LOG4J2-313
[6] Apache Software Foundation (ASF), "Log4j 2 Issues: LOG4J 2-313, jndi-lookup-plugin.patch [Attachment]," July 17, 2013, https://issues.apache.org/jira/secure/attachment/12592850/jndi-lookup-plugin.patch
[7] National Institute of Standards and Technology (NIST), National Vulnerability Database (NVD), "CVE-2021-44228 Detail," December 10, 2021, https://nvd.nist.gov/vuln/detail/CVE-2021-44228
[8] Kerner, Sean Michael, TechTarget, "Log4j explained: Everything you need to know," January 27, 2022, https://www.techtarget.com/whatis/feature/Log4j-explained-Everything-you-need-to-know
[9] Alibaba is one of the largest PRC-based technology companies, offering a variety of e-commerce, payment, and cloud technology services.
[10] ASF received this email on November 24, 2021 at 07:51 UTC. Recipients included the Apache security team's published incoming email address (security@apache.org) and the project management committee for the Apache Logging project (private@logging.apache.org).
[11] Apache Software Foundation (ASF). Response to Board request for information. April 25, 2022.
[12] Information embargos are a standard vulnerability handling practice designed to keep the details of a vulnerability private until fixes can be released. Embargoes may not always be practical, however, such as in scenarios where multiple parties need to take action.
[13] Leadership and Security team; Apache Software Foundation (ASF). Subcommittee Meeting.

2021 via two public pull requests.[14, 15] ASF opened an issue in its tracking system and committed the fix to the Log4j source code repository on December 5, 2021,[16, 17] and tagged a release candidate (Log4j-2.15.0-rc1) on December 6, 2021. [18] ASF did not release a security advisory at that time.

On December 9, 2021, the security engineer from Alibaba informed ASF via email that the vulnerability was being discussed on WeChat and provided a link to the relevant post.[19, 20] The WeChat post, made by BoundaryX, a PRC-based cybersecurity company, included a redacted screenshot of a proof of concept exploit.[21, 22] Upon receiving this information and becoming aware of subsequent public Twitter reports of ongoing exploitation, ASF escalated releasing an official fix, ahead of its original plans, and made an upgrade to version 2.15.0 available publicly on December 10, 2021.[23, 24, 25]

ASF also made the assigned Common Vulnerabilities and Exposures (CVE) identifier (CVE-2021-44228) publicly visible on December 10, 2021.[26, 27] That same day, the Cybersecurity and Infrastructure Security Agency (CISA) released a statement regarding the Log4j vulnerability.[28] Analysts at the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) assessed CVE-2021-44228 as a critical vulnerability with a Common Vulnerability Scoring System (CVSS) Base Score of 10.0, the highest score possible. This reflected the fact that exploitation of the flaw required low attack complexity, no privilege requirements, and no user interaction.[29]

The PRC government informed the Cyber Safety Review Board (CSRB, or the Board) that Alibaba notified the Ministry of Industry and Information (MIIT) of the vulnerability on December 13, 2021.[30]

Figure 1 illustrates key events from the discovery and disclosure of CVE-2021-4428 between November 24, 2021 to December 13, 2021.

---

[14] Apache Software Foundation (ASF) Log4j, GitHub, "LOG4J2-3198: Log4j2 no longer formats lookups in messages by default #607," November 29, 2021, https://github.com/apache/logging-log4j2/pull/607

[15] Apache Software Foundation (ASF) Log4j, GitHub, "Restrict LDAP access via JNDI #608," November 30, 2021, https://github.com/apache/logging-log4j2/pull/608. The pull request shows publicly visible discussions among the ASF team as the fix was developed.

[16] Apache Software Foundation (ASF) Log4j 2, Jira, "Limit the protocols JNDI can use and restrict LDAP," December 5, 2021, https://issues.apache.org/jira/browse/LOG4J2-3201

[17] Apache Software Foundation (ASF) Log4j 2, Gitbox, "Restrict LDAP access via JNDI (#608), December 5, 2021, https://gitbox.apache.org/repos/asf?p=logging-log4j2.git;h=c77b3cb

[18] Apache Software Foundation (ASF) Log4j, GitHub, "log4j-2.15.0-rc1," December 6, 2021, https://github.com/apache/logging-log4j2/releases/tag/log4j-2.15.0-rc1

[19] Apache Software Foundation (ASF). Response to Board request for information. May 15, 2022.

[20] ASF received this email on December 9, 2021 at 14:06 UTC.

[21] BoundaryX, WeChat (Weixin), "Vulnerability Risk Alert | Log4j2 Remote Code Execution Vulnerability," December 9, 2021, https://tinyurl.com/Log4j2-Vulnerability-Alert

[22] BoundaryX did not respond to the Board's request for information about where it learned of the vulnerability prior to its official public disclosure. However, its public post's analysis of the December 7, 2021 log4j-2.15.0-rc1 suggests the reasonable hypothesis that they, or someone related, discovered the vulnerability from the release candidate. The Board could not verify this hypothesis.

[23] Leadership and Security team; Apache Software Foundation (ASF). Subcommittee Meeting.

[24] Apache Software Foundation (ASF). Response to Board request for information. May 15, 2022.

[25] Leadership and Security team; Apache Software Foundation (ASF). Board Meeting.

[26] MITRE Common Vulnerabilities and Exposures (CVE), "CVE-2021-44228," December 10, 2021, https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-44228

[27] ASF is a Common Vulnerabilities and Exposures (CVE) Numbering Authority (CAN) within the MITRE CVE® Program. This role authorizes ASF to assign CVE Identifiers (IDs) for vulnerabilities found in their own products and projects for inclusion in first-time public announcements of new vulnerabilities. *Source: MITRE CVE, "Glossary: CVE Program," https://www.cve.org/ResourcesSupport/Glossary?activeTerm=glossaryCVEID# and MITRE CVE, "CVE Numbering Authority (CNA) Rules," https://www.cve.org/ResourcesSupport/AllResources/CNARules*

[28] Cybersecurity and Infrastructure Security Agency (CISA), "Apache Releases Log4j Version 2.15.0 to Address Critical RCE Vulnerability Under Exploitation," December 10, 2021, https://www.cisa.gov/uscert/ncas/current-activity/2021/12/10/apache-releases-log4j-version-2150-address-critical-rce

[29] National Institute of Standards and Technology (NIST), National Vulnerability Database (NVD), "Common Vulnerability Scoring System Calculator: CVE-2021-44228," https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2021-44228

[30] PRC government. Board Meeting. July 7, 2022. The Board received this information from an attaché at the PRC government's embassy in Washington, D.C., who delivered the message on behalf of the PRC's Ministry of Industry and Information Technology (MIIT).

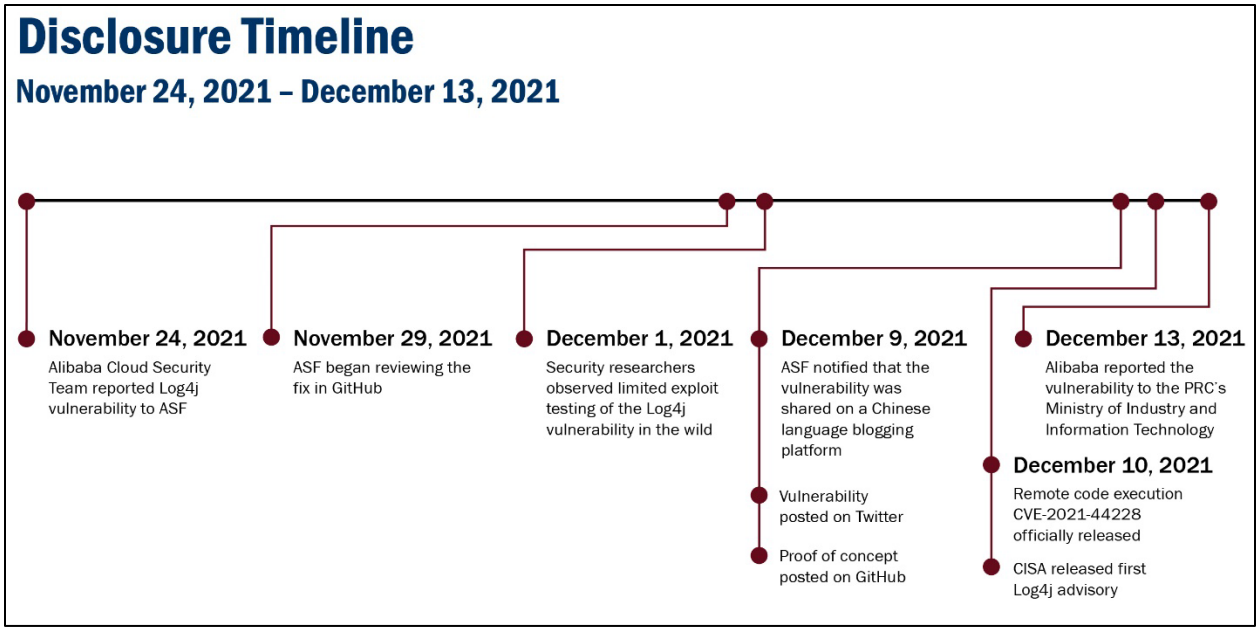

Figure 1 – Log4j Vulnerability Disclosure Timeline

Following the public disclosure of CVE-2021-44228, and widespread industry coverage, researchers discovered and reported additional vulnerabilities in Log4j to ASF. Following its standard processes, ASF triaged these reports, assigned CVE identifiers, and provided software upgrades to the community:

- CVE-2021-45046[31] – a remote code execution vulnerability (December 14, 2021) fixed in version 2.16.0;[32]
- CVE-2021-4104[33] – a remote code execution vulnerability affecting Log4j 1.2 (December 14, 2021) that could be addressed by upgrading to Log4j 2;
- CVE-2021-45105[34] – a denial-of-service (DoS) vulnerability (December 18, 2021) fixed in version 2.17.0;[35] and
- CVE-2021-44832[36] – a vulnerability that allows an attacker to modify the logging configuration file to execute remote code (December 28, 2021) fixed in version 2.17.1.[37]

1.3 EXPLOITATION

A technology services company observed the earliest known exploitation of the Log4j vulnerability over two days beginning on December 1, 2021. This company assessed the activity was consistent with the testing of

[31] National Institute of Standards and Technology (NIST), National Vulnerability Database (NVD), "CVE-2021-45046 Detail," December 14, 2021, https://nvd.nist.gov/vuln/detail/CVE-2021-45046
[32] Apache Software Foundation (ASF), "Apache Log4j Security Vulnerabilities," https://logging.apache.org/log4j/2.x/security.html
[33] National Institute of Standards and Technology (NIST), National Vulnerability Database (NVD), "CVE-2021-4104 Detail," December 14, 2021, https://nvd.nist.gov/vuln/detail/CVE-2021-4104
[34] National Institute of Standards and Technology (NIST), National Vulnerability Database (NVD), "CVE-2021-45105 Detail," December 18, 2021, https://nvd.nist.gov/vuln/detail/CVE-2021-45105
[35] Apache Software Foundation (ASF), "Apache Log4j Security Vulnerabilities," https://logging.apache.org/log4j/2.x/security.html
[36] National Institute of Standards and Technology (NIST), National Vulnerability Database (NVD), "CVE-2021-44832 Detail," December 28, 2021, https://nvd.nist.gov/vuln/detail/CVE-2021-44832
[37] Apache Software Foundation (ASF), "Apache Log4j Security Vulnerabilities," https://logging.apache.org/log4j/2.x/security.html

the Alibaba security engineer's initial proof-of-concept payload.[38, 39] In the course of our review and after examining classified and unclassified government information and industry data, the Board did not discover any additional evidence confirming further use of Log4j exploit code in the wild, including use by threat actors from the PRC, Iran, North Korea, and Russia, prior to the December 9, 2021 disclosure of the vulnerability.[40]

Numerous sources observed attempts to exploit Log4j after disclosure of the vulnerability on December 9, 2021. Security researchers and security teams also generated a large volume of vulnerability scanning activity that was difficult to distinguish from malicious activity.[41] Five days following the flaw's disclosure, Cloudflare observed 400 exploitation attempts per second,[42] totaling millions of scanning attempts to identify vulnerable systems.[43] This volume reflects SANS Institute's (SANS) observations that exploiting the flaw "is actually unbelievably simple—which makes it very, very scary at the same time."[44]

Some additional industry observations:

- Akamai assessed that approximately 57% of observed exploitation activity within the first week of public disclosure originated from known malicious actors;[45]
- a technology services company observed a spike in scanning for the vulnerability less than two hours after publication of the vulnerability;[46]
- vendors like one cybersecurity technology services company observed the use of botnets to automate the reconnaissance process to quickly identify vulnerable targets;[47]
- a cybersecurity technology services company investigated multiple ransomware incidents that leveraged the Log4j vulnerability from January 2022 through March 2022;[48]
- Check Point researchers observed nation-state threat actors exploiting the Log4j vulnerability;[49]
- Cisco Talos observed the Internet-of-Things botnet known as Mirai exploiting Log4j;[50]
- a cybersecurity technology services company attributed a high volume of initial exploitation attempts to known cybersecurity vendors and researchers;[51]
- Mandiant reported significant intrusion activity from several threat actors;[52]
- a technology services company witnessed threat actors using cryptocurrency miners and multiple ransomware payloads;[53]

---

[38] Senior executive; Technology services company. Subcommittee Meeting.
[39] Technology services company. Response to Board request for information.
[40] National Security Agency (NSA). Response to Board request for information. June 15, 2022.
[41] Chief executive; Cybersecurity technology services company. Subcommittee Meeting.
[42] Prince, Matthew (@eastdakota), Twitter, December 14, 2021, https://twitter.com/eastdakota/status/1470819030155993089
[43] Cloudflare. Subcommittee Meeting.
[44] SANS Internet Storm Center (ISC), "RCE in Log4j, Log4Shell, or How Things Can Get Bad Quickly," December 10, 2021, https://isc.sans.edu/forums/diary/RCE+in+log4j+Log4Shell+or+how+things+can+get+bad+quickly/28120/
[45] Rayasam, Aparna, Akamai, "Akamai Recommendations for Log4j Mitigation," December 16, 2021, https://www.akamai.com/blog/security/akamai-recommendations-for-log4j-mitigation
[46] Security executive; Technology services company. Board Meeting.
[47] Cybersecurity research executive; Cybersecurity technology services company. Staff Meeting.
[48] Cybersecurity technology services company. Response to Board request for information.
[49] Check Point Research, "APT35 exploits Log4j vulnerability to distribute new modular PowerShell toolkit," January 11, 2022, https://research.checkpoint.com/2022/apt35-exploits-log4j-vulnerability-to-distribute-new-modular-powershell-toolkit/
[50] Brumaghin, Edmund, Cisco Talos, "Threat Advisory: Critical Apache Log4j vulnerability being exploited in the wild," December 10, 2021, https://blog.talosintelligence.com/2021/12/apache-log4j-rce-vulnerability.html
[51] Chief executive; Cybersecurity technology services company. Subcommittee Meeting.
[52] Ackerman, Geoff et al., Mandiant, "Forged in Fire: A Survey of MobileIron Log4Shell Exploitation," March 28, 2022, https://www.mandiant.com/resources/mobileiron-log4shell-exploitation
[53] Technology services company. Response to Board request for information.

- Microsoft reported attackers attempting to leverage a previously unknown vulnerability in SolarWinds Serv-U to propagate Log4j attacks; [54] and
- Sophos observed a wave of attacks against vulnerable VMware Horizon servers beginning January 19, 2022.[55]

Log4j exploitation occurred rapidly after publication of the vulnerability,[56] so much so that exploitation in December alone earned the Log4j vulnerability a place on the Department of Homeland Security's (DHS) CISA list of Top Routinely Exploited Vulnerabilities in 2021.[57] Security researchers and vendors assess that exploitation will continue.[58, 59, 60, 61, 62]

1.4 RESPONSE

In response to the Log4j vulnerability, thousands of security professionals across the globe mobilized simultaneously to identify and mitigate hundreds of millions of potentially affected devices. One interview with the Board revealed that "no one in the industry was sleeping that weekend [following the vulnerability's announcement]—they were trying to patch millions of servers."[63] In a December 13, 2021 teleconference with industry leaders, Director Jen Easterly noted, "[the vulnerability] is one of the most serious I've seen in my entire career, if not the most serious."[64] Industry experts and reporters echoed her sentiments.

Communications and Public Guidance

Immediately following the disclosure of the Log4j vulnerability, software developers and cybersecurity professionals globally used formal and informal communication channels to share mitigation tactics and provide guidance to the public.

Many interviewed stakeholders indicated one of their earliest, if not their first, notifications of the vulnerability came from social media platforms, especially Twitter,[65, 66, 67] where the broader security community shared vulnerability information and emerging indicators of compromise (IOC). Individual accounts also shared exploitation variants, obfuscation and defense evasion techniques, and other trends to enable responders to adjust defensive measures and deter potential attacks. Multiple interviewees told the Board that Twitter was a valuable resource for global events of this type.[68, 69]

---

[54] Microsoft Security, "Guidance for preventing, detecting, and hunting for exploitation of the Log4j 2 vulnerability," December 19, 2021, https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/

[55] Gallagher, Sean and Szappanos, Gabor, Sophos, "Horde of miner bots and backdoors leveraged Log4J to attack VMware Horizon servers," March 29, 2022, https://news.sophos.com/en-us/2022/03/29/horde-of-miner-bots-and-backdoors-leveraged-log4j-to-attack-vmware-horizon-servers/

[56] Wisniewski, Chester, Sophos, "Log4Shell: No Mass Abuse, But No Respite, What Happened?" January 24, 2022, https://news.sophos.com/en-us/2022/01/24/log4shell-no-mass-abuse-but-no-respite-what-happened/

[57] Cybersecurity and Infrastructure Security Agency (CISA), "Alert (AA22-117A): 2021 Top Routinely Exploited Vulnerabilities," April 27, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-117a

[58] Newman, Lily Hay, Wired, "The Log4J Vulnerability Will Haunt the Internet for Years," December 13, 2021, https://www.wired.com/story/log4j-log4shell/

[59] Cybersecurity technology services company. Response to Board request for information.

[60] Cybersecurity technology services company. Response to Board request for information.

[61] Cybersecurity Action Team, Google, "Threat Horizons," February 2022, https://services.google.com/fh/files/misc/gcat_threathorizons_full_feb2022.pdf

[62] Microsoft Security, "Guidance for preventing, detecting, and hunting for exploitation of the Log4j 2 vulnerability," December 19, 2021, https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/

[63] Senior executive; Cybersecurity technology services company. Subcommittee Meeting.

[64] Starks, Tim; CyberScoop, "CISA Warns 'Most Serious' Log4j Vulnerability Likely to Affect Hundreds of Millions of Devices," December 13, 2021, https://www.cyberscoop.com/log4j-cisa-easterly-most-serious/

[65] Federal Chief Information Security Officer (CISO). Response to Board request for information.

[66] Senior executive; Technology services company. Subcommittee Meeting.

[67] Chief Information Security Officer (CISO); Technology services company. Board Meeting.

[68] Federal Chief Information Security Officer (CISO). Response to Board request for information.

[69] Technology services company. Response to Board request for information.

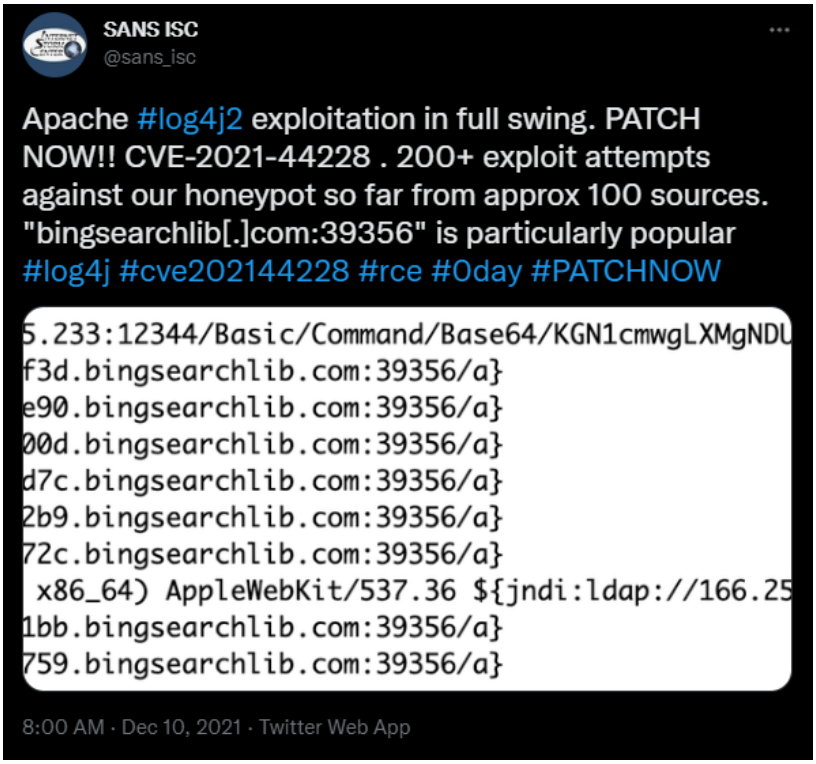

Figure 2 – SANS Internet Storm Center (ISC) detailing the scale of Log4j exploit attempts on December 10, 2021

U.S. Government Coordination

All U.S. government agencies had a role in responding to Log4j: protecting their own networks; tracking potential malicious activity; or prompting key constituencies to act. However, the Board's review largely focused on CISA and its role in protecting federal infrastructure, and the Office of the Federal Chief Information Security Officer.

On December 10, 2021, one day after the public disclosure of the vulnerability, CISA issued a statement highlighting the ASF advisory and encouraged users and administrators to upgrade their systems or apply mitigations immediately.[70] On December 17, CISA released Emergency Directive (ED) 22-02, which detailed mitigation measures for vulnerable products and patch prioritization recommendations, and required civilian Executive Branch agencies to address Log4j vulnerabilities within two weeks.[71] In the days following the disclosure, CISA focused on facilitating collaboration with trusted partners, such as its efforts to understand mitigations for Industrial Control Systems (ICS) vendors with Carnegie Mellon's Vulnerability Information and Coordination Environment (VINCE) software vulnerability team.[72]

CISA also tapped into the newly established Joint Cyber Defense Collaborative (JCDC),[73] which facilitated the collection, organization, and consolidation of data to determine the impact of the vulnerability and support the development of comprehensive remediation. In interviews with the Board, a number of stakeholders reported

[70] Cybersecurity and Infrastructure Security Agency (CISA), "Apache Releases Log4j Version 2.15.0 to Address Critical RCE Vulnerability Under Exploitation," December 10, 2021, https://www.cisa.gov/uscert/ncas/current-activity/2021/12/10/apache-releases-log4j-version-2150-address-critical-rce
[71] Cybersecurity and Infrastructure Security Agency (CISA), "*Emergency Directive 22-02 Mitigate Apache Log4j Vulnerability*," December 17, 2021, https://www.cisa.gov/emergency-directive-22-02
[72] Goldstein, Eric; Cybersecurity and Infrastructure Security Agency (CISA). Board Meeting. February 25, 2022.
[73] Cybersecurity and Infrastructure Security Agency (CISA), "Joint Cyber Defense Collaborative (JCDC)," https://www.cisa.gov/jcdc

that the JCDC was an important catalyst for information sharing to address the threat.[74, 75, 76] CISA received 17 threat analyses from JCDC members that it would not have otherwise seen until days later, when those members eventually published their products.[77] Notably, some material that JCDC members provided to CISA was not publicly released, but CISA was still able to access and use this information to better inform its products, guidance, and analysis.[78]

To coordinate and communicate with external partners in real time during the Log4j event, CISA established Slack channels. One JCDC member reported to the Board that these Slack channels were beneficial for bi-directional information sharing between industry and government stakeholders, especially early in the vulnerability response.[79] CISA set up several channels that varied in purpose and participants; one channel was for sharing threat information (e.g., tactics, techniques, and procedures (TTPs) and IOCs) and analysis among JCDC's Alliance partners and other key technology companies. CISA also created a channel for related collaboration across JCDC's U.S. government partners.[80]

Before issuing ED 22-02, CISA launched two community resources on December 13, 2021:

- a centralized knowledge management website of high-level, executive-level, and technical products, including pre-vetted information from trusted partners;[81, 82] and
- a GitHub repository[83] with an extensive list of vulnerable products and components to help responders understand where the Log4j software resided within their environments, along with associated remediation recommendations.[84]

CISA noted that it shared guidance from third parties that it vetted and identified as credible due to their reputation and prior work. Due to the urgency of the situation, CISA shared other unvalidated third-party resources and encouraged readers to independently verify the information.[85] CISA worked directly with researchers and vendors to identify and catalog vulnerable products within a well-received public GitHub repository.[86, 87, 88]

CISA's response provided defenders with specific and comprehensive guidance for vulnerability management, including patch prioritization. Stakeholders provided positive feedback to the Board about the utility of CISA's guidance, saying it provided a trusted source for direction and specific resources.[89] However, some

---

[74] Federal Chief Information Security Officer (CISO). Response to Board request for information.
[75] Senior executive; Cybersecurity technology services company. Subcommittee Meeting.
[76] The Log4j and SolarWinds events emphasized the importance of industry and federal collaboration. Active participation across these groups, including official CISA and vendor advisories, helped drive results by informing organizations of event criticality and furnishing continuous mitigation advice. *Source: Mandia, Kevin, FireEye, "FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community," December 8, 2020, https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html; Cybersecurity and Infrastructure Security Agency (CISA), "Emergency Directive 21-01 – Mitigate SolarWinds Orion Code Compromise, https://www.cisa.gov/emergency-directive-21-01*
[77] Goldstein, Eric; Cybersecurity and Infrastructure Security Agency (CISA). Board Meeting. February 25, 2022.
[78] Cybersecurity and Infrastructure Security Agency (CISA). Response to Board request for information. May 27, 2022.
[79] Senior executive; Cybersecurity technology services company. Subcommittee Meeting.
[80] Cybersecurity and Infrastructure Security Agency (CISA). Response to Board request for information. May 6, 2022.
[81] Cybersecurity and Infrastructure Security Agency (CISA), "CISA Creates Webpage for Apache Log4j Vulnerability CVE-2021-44228," December 13, 2021, https://www.cisa.gov/uscert/ncas/current-activity/2021/12/13/cisa-creates-webpage-apache-log4j-vulnerability-cve-2021-44228
[82] Cybersecurity and Infrastructure Security Agency (CISA), "Apache Log4j Vulnerability Guidance," https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance
[83] The Cybersecurity and Infrastructure Security Agency (CISA) noted that Kevin Beaumont and personnel from the National Cyber Security Centre of the Netherlands (NCSC-NL) provided critical input to CISA in standing up the GitHub repository of impacted products. Many other researchers submitted impacted products to the repository subsequent to its launch. *Source: Goldstein, Eric; Cybersecurity and Infrastructure Security Agency (CISA). Board Meeting. February 25, 2022.*
[84] Cybersecurity and Infrastructure Security Agency (CISA), GitHub, "log4j-affected-db," December 13, 2021, https://github.com/cisagov/log4j-affected-db
[85] Cybersecurity and Infrastructure Security Agency (CISA), "Alert AA21-356A: Mitigating Log4Shell and Other Log4j-Related Vulnerabilities," December 22, 2021. https://www.cisa.gov/uscert/ncas/alerts/aa21-356a
[86] Goldstein, Eric; Cybersecurity and Infrastructure Security Agency (CISA). Board Meeting. February 25, 2022.
[87] Cybersecurity and Infrastructure Security Agency (CISA). Response to Board request for information. May 6, 2022.
[88] Leadership and Security team; Apache Software Foundation (ASF). Board Meeting.
[89] Federal Chief Information Security Officer (CISO). Response to Board request for information.

stakeholders noted that unvalidated social media sources occasionally published information before credible government and industry sources issued guidance.

Other U.S. government agencies also created alerts and provided guidance for Log4j mitigation. On December 15, 2021, the Federal Bureau of Investigation (FBI) published a message encouraging victims to report any malicious activity or victim compromise.[90] CISA, the FBI, the National Security Agency (NSA), and international cybersecurity counterparts from Australia, Canada, New Zealand, and the United Kingdom (U.K.) published a joint advisory with technical details, mitigations, and resources for organizations using Log4j products.[91] The Federal Trade Commission (FTC) amplified CISA's guidance through a blog post, declaring that "[t]he FTC intends 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 in the future."[92] The Department of Defense (DoD) also published a memorandum on January 24, 2022 that cited two fundamental concerns surrounding the use of open source software: supply chain risk management for externally maintained code in critical DoD systems as potential paths for introduction of malicious code; and the disclosure of key innovations via imprudent sharing of code developed for DoD systems for adversary benefit.[93]

See Appendix D for communications from U.S. and foreign governments, the private sector, and the media.

Case Studies: Other Government Responses to Log4j

The Board engaged representatives from government cybersecurity agencies in Israel and the United Kingdom to share notable features of their responses to the Log4j vulnerability

Israel	United Kingdom
The Israel National Cyber Directorate (INCD) leveraged internal and perimeter vulnerability scanners alongside a comprehensive configuration management database (CMDB) and internet service provider (ISP) data to filter, aggregate, correlate, and enrich data for providing information about the vulnerability. While INCD observed approximately 3 million attempts to exploit the Log4j vulnerability, INCD representatives attributed their ability to quickly remediate successful exploitation incidents to having the right people in the right place with the right resources.[94] In particular, INCD noted that it closed the vulnerability relatively quickly because it aligned dedicated resources to its critical infrastructure organizations.	After the critical Microsoft Exchange vulnerabilities in 2021, the U.K.'s National Cyber Security Centre (NCSC-UK) integrated new processes to improve future vulnerability management guidance, which it leveraged throughout the Log4j event. The NCSC-UK used a newly implemented vulnerability scoring and categorization framework (developed to complement its existing incident categorization matrix) to determine the need for response and coordination across government and law enforcement resources. In addition to providing responders with a kit that contained mitigation and remediation guidance and critical vulnerability advice for boards, the NCSC-UK also hosted an "ask me anything" session to facilitate real-time response endeavors.[95]

Organizational Responses

Generally, organizations that responded most effectively to the Log4j event understood their systems' use of Log4j and had technical resources and mature processes to manage assets,[96] absorb new information and assess the potential risk, and mobilize the entire organization and key partners to action.[97] In many cases,

[90] Federal Bureau of Investigation (FBI), "Seeking Victims of Log4j Vulnerability," December 15, 2021, https://www.fbi.gov/resources/victim-services/seeking-victim-information/seeking-victims-of-log4j-vulnerability
[91] Cybersecurity and Infrastructure Security Agency (CISA), "Alert (AA21-356A): Mitigating Log4Shell and Other Log4j-Related Vulnerabilities," December 22, 2021, https://www.cisa.gov/uscert/ncas/alerts/aa21-356a
[92] Federal Trade Commission (FTC), "FTC warns companies to remediate Log4j security vulnerability," January 4, 2022, https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability
[93] Department of Defense (DoD), "Software Development and Open Source Software," January 24, 2022, https://dodcio.defense.gov/Portals/0/Documents/Library/SoftwareDev-OpenSource.pdf
[94] Senior director; Foreign government cyber organization. Subcommittee Meeting.
[95] Senior director; Foreign government cyber organization. Subcommittee Meeting.
[96] Chief Information Security Officer (CISO); Critical infrastructure sector company. Subcommittee Meeting.
[97] Senior executive; Critical infrastructure sector company. Subcommittee Meeting.

however, a lack of awareness and understanding of Log4j, insufficient resources, or lack of vendor upgrades hampered organizational response to the vulnerability.[98]

Many security engineers reported addressing the complexity or impossibility of upgrading Log4j immediately by using a wide variety of mitigation actions,[99, 100] especially when patches for third-party products were unavailable. These actions included:

- egress filtering of network traffic from systems utilizing vulnerable Log4j code;
- deleting the JndiLookup.class file containing the vulnerable code;
- patching or disabling sections of vulnerable code, including modifying running systems by applying hot patches;
- blocking possible attack traffic by configuring Web Application Firewalls (WAF) to limit exploit queries; and
- physically removing affected assets from the network until they could be upgraded.

[98] Senior director; Foreign government cyber organization. Subcommittee Meeting.
[99] Federal Chief Information Security Officer (CISO). Response to Board request for information.
[100] Federal Chief Information Security Officer (CISO). Subcommittee Meeting.

SECTION 2 – FINDINGS AND CONCLUSIONS

The Board's findings and conclusions are the result of its independent review. These findings and conclusions are based on information gleaned from literature searches, interviews, requests for information, and analysis of public, private, and government-source information. The Board relied upon the voluntary participation of numerous organizations affected by the Log4j vulnerability.

The findings and conclusions in this section are not intended to assign blame or fault to any individual or collective parties, but rather to highlight opportunities where the community can understand lessons and apply safety improvements for the future.

2.1 SUMMARY OF FINDINGS

The Log4j event illustrates how counterintuitive cybersecurity defense can be, for both individual enterprises and for the ecosystem as a whole. Many things went "right": ASF had a well-established software development lifecycle with clear roles for vetting, testing, and approval of new code; security researchers followed generally accepted steps of coordinated disclosure; ASF quickly recognized the criticality of the problem and made upgrades available; vendors and governments rapidly produced guidance, tools, and threat information; and the whole ecosystem rallied behind a collective sense of urgency.[101, 102] However, organizations still struggled to respond to the event, and in fact, the Board found that many organizations have still not fully patched vulnerable instances of Log4j.

The Board found that software developers, maintainers, vulnerability response teams, and the U.S. government commonly made risk trade-offs about software use and integration. For example, organizations made the decision to use Log4j, rather than develop a logging framework from scratch. Similarly, organizations make decisions to use software from an established organization (e.g., ASF) based on its mature and vetted processes. The Log4j event highlighted fundamental adoption gaps in vulnerability response practices and overall cybersecurity hygiene. These gaps highlighted challenges in raising awareness within organizations; coordinating trusted and authoritative sources of information; mitigating at scale; measuring the enormity of the risk; and synchronizing the understanding of threats and corresponding defensive action.[103]

The fundamentals of Enterprise Risk Management, described in this section, are foundational tools that enable organizations to locate affected software assets, rapidly identify risks to business operations, upgrade vulnerable software, and monitor for malicious activity.[104]

---

[101] Federal Chief Information Security Officer (CISO). Subcommittee Meeting.

[102] Recent coordination efforts between researchers, vendors, and the federal government demonstrate enhanced agility and alignment across industry verticals. This observation poses an opportunity for experts to leverage their skill set (e.g., software development, threat intelligence, and similar skills) to identify risks and improve communal trust across sectors via responsible disclosure. As observed through both the Log4j and SolarWinds events, this also enables authoritative sources to promote awareness and facilitate vulnerability management efforts to address emergent risks. *Source: Mandia, Kevin, FireEye, "FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community," December 8, 2020, https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html; Cybersecurity & Infrastructure Security Agency (CISA), "Emergency Directive 21-01 – Mitigate SolarWinds Orion Code Compromise, https://www.cisa.gov/emergency-directive-21-01*

[103] Remediation efforts following the SolarWinds supply chain attack emphasized the need for improved public-private engagement and information sharing. As a result, CISA established the Joint Cyber Defense Collaborative (JCDC) in December 2021, which proved beneficial throughout the Log4j event. *Source: U.S. Government Accountability Office (GAO), "Federal Response to SolarWinds and Microsoft Exchange Incidents," January 2022, https://www.gao.gov/assets/gao-22-104746.pdf*

[104] In the days following the disclosure of the Log4j vulnerability, CISA and other community defenders developed various specialized tools to identify vulnerable Log4j libraries. The SolarWinds supply chain attack also demonstrated the importance of achieving system-wide visibility through comprehensive asset management, continuous monitoring, and threat detection capabilities. The GAO cited the government's ability to move fast with specialized tools to detect compromised software. For example, CISA's Cloud Forensics team publicly released "Sparrow" in December 2020 to help uncover compromised accounts and applications within Azure and Microsoft 365 environments. Both events emphasize the importance of tooling to enable asset discovery, vulnerability management, and threat detection. *Source: U.S. Government Accountability Office (GAO), "Federal Response to SolarWinds and Microsoft Exchange Incidents," January 2022, https://www.gao.gov/assets/gao-22-104746.pdf*

2.2 CONTRIBUTING FACTORS OF THE VULNERABILITY

At a technical level, the introduction of the JNDI lookup plugin support "which could be exploited by an attacker due to the way Log4j interacts with JNDI without properly validating all requests"[105] as outlined in Section 1.1 –Discovery and Disclosure led to the Log4j vulnerability. However, a number of factors amplified the scale, complexity, and risk level of the vulnerability:

- Log4j is routinely embedded in other software components, often unknown at later levels of integration or system operation, making it a difficult vulnerability to identify using common scanning approaches;
- the Log4j framework is incorporated into thousands of software components globally,[106] and many of the nation's critical infrastructure and government systems rely on it;
- consistent with industry convention, the Log4j and ASF teams do not manage or know who uses the software they produce, or how it is eventually used;
- the Log4j vulnerability is easy for attackers to exploit and affords a high degree of system control to an attacker once exploited.[107, 108]

The Board also found specific challenges associated with maintaining open source projects like Log4j, which generally rely on volunteer teams and do not necessarily have dedicated security resources throughout the Software Development Lifecycle.[109] Open source projects generally do not have dedicated coordinated vulnerability disclosure and response teams that investigate root causes of reported vulnerabilities and work to bring them to resolution. Open source projects like Log4j often also develop code "in the open," where security changes are publicly visible as they are being developed. This suggests that advisories and community response may need to be activated concurrently with any fixes to narrow the window for malicious exploitation prior to the official patch being available for defenders.[110] See Appendix E for the Board's observations of the open source software ecosystem during the Log4j event.

These factors created a perilous combination: an enormous attack surface vulnerable to exploitation; vulnerability response teams that often could not identify where the vulnerable code could be found in their systems; and a vulnerability that is easily exploited to grant significant unauthorized access to systems, including sensitive systems used to support critical infrastructure and federal government operations.

The Board also examined whether the Log4j vulnerability could have been prevented or caught earlier, particularly whether the introduction of the JNDI lookup plugin support in 2013 would have resulted in unintended exploitability of the added functionality. The Board concluded that a focused review, performed by someone with sufficient experience with the security implications of adding the JNDI support, could have identified the unintended functionality (i.e., the vulnerability). Unfortunately, the resources to perform such a review were not available to the volunteer developers who led this open-source project in 2013.[111, 112]

---

[105] Kerner, Sean Michael, TechTarget, "Log4j explained: Everything you need to know," January 27, 2022, https://www.techtarget.com/whatis/feature/Log4j-explained-Everything-you-need-to-know

[106] The Log4j and SolarWinds events both revealed the far-reaching attack surface and potential damage that can result from a problem found within a widely distributed technology. *Source: Federal Agency. Response to Board request for information.*

[107] Chief executive; Cybersecurity technology services company. Subcommittee Meeting.

[108] Similar to consequences of the Log4j 2 vulnerability, the SolarWinds supply chain compromise enabled threat actors to gain initial access to several target environments, move throughout their systems, and deploy multi-staged attacks. *Source: Herr, Trey et al., The Atlantic Council, "Broken Trust: Lessons from Sunburst," March 2021, https://www.atlanticcouncil.org/wp-content/uploads/2021/03/BROKEN-TRUST.pdf*

[109] Manager; Non-profit organization. Board Meeting.

[110] Attackers "reverse engineering" releases (in compiled code and patches) to look for vulnerabilities is a well-known problem. For example in May 2022 CISA released Emergency Directive 22-03, citing that attackers had reverse engineered VMWare updates within 48 hours of their release. *Source: Cybersecurity and Infrastructure Security Agency (CISA), Emergency Directive 22-03 Mitigate VMWare Vulnerabilities, May 18, 2022, https://www.cisa.gov/emergency-directive-22-03*

[111] Manager; Software Engineering Institute (SEI), Carnegie Mellon University (CMU). Subcommittee Meeting.

[112] Software developer. Subcommittee Meeting.

The ASF developers conveyed to the Board that automated security testing would not have caught this specific vulnerability, though they noted that an extensive code audit might have identified the issue.[113] The Log4j developers might not have introduced the vulnerability in 2013 if they had had access at the time to training in secure coding practices consistent with established secure development lifecycle tools and techniques.[114] A technology services company seconded that position and suggested that security-oriented design reviews, threat models, and security audits may have prevented events such as Log4j.[115]

Ultimately, even if the Log4j developers or others had identified the flaw in published versions of Log4j prior to November 2021, the community would still have had to respond as outlined in this report. The Board also found that the only way to reduce the likelihood of risk to the ecosystem caused by vulnerabilities in Log4j, and other widely used open source software, is to ensure that code is developed pursuant to industry-recognized secure coding practices and an attendant audit by security experts. The open source community, which is volunteer-based, would need sustained financial support and expertise to make this possible.

2.3 ENTERPRISE RISK MANAGEMENT

After disclosure of the Log4j vulnerability, organizations had to rapidly assess and manage their potential risk, at both a technical and business level.[116] Generally, the Board found that organizations that responded most effectively to the Log4j event already had technical resources and mature processes in place to identify vulnerable assets, absorb new information, assess potential risk, and mobilize their entire organization and key partners to action. See Appendix F for a summary of the Board's insights on effective practices that organizations leveraged when managing the Log4j event.

Most modern security frameworks call out these activities, such as:

- application of technologies and processes that enable the management of and visibility into hardware, software, and systems;
- activation of existing incident crisis, or vulnerability management plans, which clearly define responsibilities and for which staff has been trained;
- ongoing risk management processes that identify business/mission-critical systems, data application, outsourced risk management partners, and establish traceable mitigation strategies; and
- plans for internal and external communication methods to inform leadership, internal teams, and customers.

More security-mature organizations also mobilized existing and ad hoc teams to:

- bring together groups such as security operations, information technology (IT) operations, penetration testing, vulnerability management, threat intelligence, and product security to identify enterprise weak spots, compare them to external attacker trends, and mobilize defenses; and

[113] Leadership and Security team; Apache Software Foundation (ASF). Board Meeting.
[114] Manager; Non-profit organization. Board Meeting.
[115] Technology services company. Response to Board request for information.
[116] The evolution of recent cybersecurity events indicates their inherently dynamic nature – assessments of impact rely on emergent properties. Responders were unaware of the scope of required patching and mitigation following the discovery of CVE-2021-44228. Similarly, as revealed in the SolarWinds supply chain attack, organizations did not understand the variety and breadth of second and third-stage compromises until well after FireEye reported the breach. *Source: Mandiant, "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor," December 13, 2020, https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor; Rapid7, "2021 Vulnerability Intelligence Report," March 28, 2022, https://information.rapid7.com/rs/411-NAK-970/images/Rapid7%202021%20Vulnerability%20Intelligence%20Report.pdf*

- create coordination teams to oversee Log4j-related activities across the organization and to participate in active outreach to third-party service providers, the general public, and government entities.[117, 118]

Many organizations made use of mitigations described in Section 1.4 – Response, subsection Organizational Responses (such as turning off affected systems or using WAFs). While these were helpful in the short term, they did not correct the underlying issues, or were superseded by later guidance that required additional resources. Some mitigations were more drastic (including removing systems from production) and had direct impact on mission. However, as ASF released various upgrades for Log4j, organizations focused on upgrading their systems, due to the nature of the vulnerability.[119]

Many organizations depended on the responsiveness of their vendors to understand and remediate the vulnerability.[120] Some organizations still harbor concerns, despite vendors reporting having implemented updates, due to the interdependencies between different applications and components.[121]

Industry experts have called for increased automation to help organizations identify vulnerable software and execute Enterprise Risk Management at scale, but they also recognize that cataloging software components at this depth can be prohibitively labor intensive. Solutions to enable these necessary capabilities do not exist.

The Role of Software Bills of Materials

Software Bills of Materials (SBOMs) provide a list of components included in software, and theoretically should enable organizations to identify vulnerable software components in their environments.[122] The Board spoke with representative groups for organizations currently using SBOMs in their environments, and none reported having leveraged them to identify vulnerable deployments of Log4j.

As designed today, SBOMs are limited, for example by variances in field descriptions and a lack of version information about catalogued components, and lack of automation on the consumption end due to these variances. Addressing SBOM standardization gaps would support a faster software supply chain vulnerability response.

2.4 ECOSYSTEM RISK MANAGEMENT

During the Log4j event, risk management activities across the ecosystem impacted individual organizations' response efforts. For example, all parties benefited when a trusted entity, CISA, raised an alarm and provided mitigations, such as its joint Log4j cybersecurity advisory[123] and ED 22-02.[124] On the other hand, the ecosystem also contributed to "noise" and uncertainty in the early days of the vulnerability disclosure, leading to an overwhelming amount of information.

Based on the severity of the Log4j vulnerability, all enterprises needed to rapidly assess the potential risk to their business operations and develop and execute a plan of action. The U.S. government also needed to understand and manage the overall risk to the total U.S. cyber ecosystem. This required integration of information across the full range of threats, vulnerabilities, and potential consequences. It also required the ability to define the risk and spur action across the United States, especially within critical infrastructure and government, including national security functions.

---

[117] Technology services company. Response to Board request for information.
[118] Technology services company. Response to Board request for information.
[119] Senior executive; Cybersecurity technology services company. Subcommittee Meeting.
[120] Vijayan, Jai, Dark Reading, "Why Log4j Mitigation Is Fraught With Challenges," December 16, 2021, https://www.darkreading.com/application-security/why-log4j-mitigation-is-fraught-with-challenges
[121] Chief executive; Non-profit organization. Subcommittee Meeting.
[122] National Telecommunications and Information Administration (NTIA), "Comments on Software Bill of Materials Elements and Considerations," June 21, 2021, https://www.ntia.gov/other-publication/2021/comments-software-bill-materials-elements-and-considerations
[123] Cybersecurity and Infrastructure Security Agency (CISA), "Alert (AA21-356A): Mitigating Log4Shell and Other Log4j-Related Vulnerabilities," December 22, 2021, https://www.cisa.gov/uscert/ncas/alerts/aa21-356a
[124] Cybersecurity and Infrastructure Security Agency (CISA), "*Emergency Directive 22-02 Mitigate Apache Log4j Vulnerability*," December 17, 2021, https://www.cisa.gov/emergency-directive-22-02

Even before the Log4j vulnerability disclosures, CISA had taken important steps to drive network defender attention toward broader risk management of known security vulnerabilities. On November 3, 2021, CISA issued Binding Operational Directive (BOD) 22-01 – *Reducing the Significant Risk of Known Exploited Vulnerabilities (KEVs)*.[125] Based on persistent cyber campaigns threatening the public and private sectors, this publication established a catalog of KEVs representing significant risk to the federal enterprise.[126] The directive required federal agencies to take three actions:

- review and update agency internal vulnerability management procedures;
- remediate each vulnerability; and
- report on the status of vulnerabilities listed in the catalog.

CISA updated the catalog on December 10, 2021 to include Log4j (CVE-2021-44228). The catalog established a clear U.S. government-wide policy and an expectation of action and reporting. It also brought specific operational priority to ongoing federal activities to complement technology improvement and compliance programs.

Other U.S. federal agencies chose to amplify or highlight CISA's resources and guidance. For example, the FTC issued a blog post citing CISA's guidance and resources for managing the risk around Log4j. This blog post outlined the FTC's intent to use its full legal authority to pursue companies that failed to take reasonable steps to protect consumer data due to exposure resulting from Log4j. Anecdotal reports suggest this blog drove significant mitigation activity among organizations concerned with the FTC's potential enforcement actions.[127] While this communication was not coordinated directly with CISA, it highlights how regulatory agencies and CISA can benefit from each others' expertise and authorities. CISA is the authoritative federal voice on how to reduce risk from a severe vulnerability like Log4j. Regulators (whether federal or state) do not generally have CISA's level of cybersecurity expertise, but can use their significant enforcement authorities to drive compliance with CISA's guidance among their regulated communities. This results in improved uptake of CISA's recommendations, and thus improved overall national cybersecurity.

Ecosystem Risks Inherent in the PRC's Regulatory Regime and Sanctions Against Alibaba

The global community benefited from the engineer at Alibaba following recognized practices for coordinated vulnerability disclosure.

[125] Cybersecurity and Infrastructure Security Agency (CISA), "Binding Operational Directive 22-01 – *Reducing the Significant Risk of Known Exploited Vulnerabilities*," November 3, 2021, https://www.cisa.gov/binding-operational-directive-22-01

[126] Similar to CISA and Office of Management and Budget's (OMB) incident management of Log4j, federal agency coordination garnered positive results when responding to the SolarWinds supply chain attack. These events demonstrated the government's efforts surrounding centralized reporting and effective communication practices. For example, NTIA's Communication Supply Chain Risk Information Partnership (C-SCRIP) coordinates incident response and threat intelligence between several federal agencies, and CISA's National Cybersecurity and Communications Integration Center (NCCIC) coordinates government risk management efforts. *Source: U.S. Government Accountability Office (GAO), "Federal Response to SolarWinds and Microsoft Exchange Incidents," January 2022, https://www.gao.gov/assets/gao-22-104746.pdf; Herr, Trey et al., The Atlantic Council, "Broken Trust: Lessons from Sunburst," March 2021, https://www.atlanticcouncil.org/wp-content/uploads/2021/03/BROKEN-TRUST.pdf*

[127] Cybersecurity and Infrastructure Security Agency (CISA). Response to Board request for information. May 27, 2022.

The PRC government informed the Board that Alibaba reported the vulnerability to the PRC's Ministry of Industry and Information Technology on December 13, 2021.[128, 129] This report to MIIT appears to be 19 days after the Alibaba security engineer private disclosure of the vulnerability to ASF, and 17 days after a deadline stipulated in Article 7.2 of MIIT's *Regulations on the Management of Security Vulnerabilities of Network Products*, which would have obligated Alibaba to report vulnerabilities in its own products (i.e., its own products that incorporate Log4j).[130] Starting December 22, 2021, several Western and Chinese-language media sources reported that MIIT suspended Alibaba from a cybersecurity threat information sharing platform partnership for failing to report the Log4j vulnerability to MIIT in a timely manner.[131, 132, 133, 134] Because the PRC government has not publicly provided a detailed explanation of any sanctions, and MIIT's response to the Board's official request for information did not address this specific matter, the Board was unable to verify the rationale for the sanctions.

Independent of a possible sanction against Alibaba, the Board noted troubling elements of MIIT's regulations governing disclosure of security vulnerabilities. The requirement for network product providers to report vulnerabilities in their products to MIIT within two days of discovery could give the PRC government early knowledge of vulnerabilities before vendor fixes are made available to the community. The Board is concerned this will afford the PRC government a window in which to exploit vulnerabilities before network defenders can patch them. This is a disturbing prospect given the PRC government's known track record of intellectual property theft,[135] intelligence collection,[136] surveillance of human rights activists and dissidents,[137] and military cyber operations.[138]

---

[128] PRC government. Board Meeting. July 7, 2022. In response to a written Board request about the Log4j event and the PRC government's involvement in it, an attaché from the PRC embassy in Washington, D.C. offered the following verbal statement on behalf of the PRC Ministry of Industry and Information Technology, but would not answer follow up questions:

> Cybersecurity is a common challenge faced by all countries and maintaining cybersecurity requires the joint participation of the public and private sectors of all countries. On December 13, 2021 Alibaba called and reported to the Ministry of Industry and Information Technology of the PRC (MIIT) that it had discovered a security vulnerability in the Apache Log4j 2 component and informed the Apache Software Foundation of the United States. Based on the vulnerability, patches released by Apache, MIIT issued network and cybersecurity risk alerts to the society. Alibaba took its own technical capability to take the lead in discovering the vulnerability and reporting it to the relevant software providers is worthy of recognition. The Chinese government encourages and supports capable enterprises to promptly notify network providers to patch vulnerabilities and enhance productive security in accordance with the open source community vulnerability information disclosure rules after discovering vulnerabilities. We also encourage enterprises to share cyber threat information and improve the level of provision and response to cyber threats of all parties so as to build a more secure and [inaudible] open cyberspace. Relevant information can be found on the website, including that of the MIIT.

[129] Ministry of Industry and Information Technology (MIIT), "Network security risk reminder about major security vulnerabilities in Apache Log4j2 components" (translated), December 17, 2021, https://www.miit.gov.cn/xwdt/gxdt/sjdt/art/2021/art_7587d13959e24aeb86887f7ef60d50d3.html

[130] Ministry of Industry and Information Technology (MIIT) and State Internet Information Office of the Ministry of Public Security of the People's Republic of China, "Notice of the Ministry of Industry and Information Technology and the State Internet Information Office of the Ministry of Public Security on Issuing the *Regulations on the Management of Security Vulnerabilities of Network Products*" (translated), July 13, 2021, http://www.cac.gov.cn/2021-07/13/c_1627761607640342.htm

[131] Liyang, Wu, 21st Century Business Herald, "Apache安全漏洞全球发酵 工信部暂停阿里云合作单位, Log4j2问题影响几何?," December 22, 2021, https://sfccn.com/article/20211222/herald/NzU4LTQ0NDEzMA==.html

[132] British Broadcasting Corporation (BBC), "Chinese regulator pauses partnership with Alibaba," December 23, 2021, https://www.bbc.com/news/technology-59760486

[133] Reuters, "China regulator suspends cyber security deal with Alibaba Cloud," December 21, 2021, https://www.reuters.com/world/china/china-regulator-suspends-cyber-security-deal-with-alibaba-cloud-2021-12-22/

[134] Lin, Liza and Uberti, David, The Wall Street Journal, "Alibaba Employee First Spotted Log4j Software Flaw but Now the Company Is in Hot Water With Beijing," December 22, 2021, https://www.wsj.com/articles/china-halts-alibaba-cybersecurity-cooperation-for-slow-reporting-of-threat-state-media-says-11640184511

[135] Financial Times, "America is struggling to counter China's intellectual property theft," April 18, 2022, https://www.ft.com/content/1d13ab71-bffd-4d63-a0bf-9e9bdfc33c39

[136] Cheng, Dean, The Heritage Foundation, Congressional Testimony, "The PRC and Intelligence Gathering: Unconventional Targets and Unconventional Methods," December 12, 2018, https://www.judiciary.senate.gov/download/12-12-18-cheng-testimony

[137] Freedom House, "China: Transnational Repression Case Study," February 2021, https://freedomhouse.org/report/transnational-repression/china

[138] Cybersecurity and Infrastructure Security Agency (CISA), "Alert (AA21-200B) Chinese State-Sponsored Cyber Operations: Observed TTPs," July 19, 2021, https://www.cisa.gov/uscert/ncas/alerts/aa21-200b

Furthermore, Article 9.6 of the MIIT regulations includes a provision prohibiting organizations or individuals from publicly disclosing vulnerabilities during "major national events" without the consent of the Ministry of Public Security (MPS). This regulation does not appear to prevent disclosure of a vulnerability to affected parties responsible for creating a fix, but depending on the domicile of that party, it may create circumstances where the PRC government can prohibit a public disclosure under vague, lightly-defined conditions. This could potentially prolong the period in which the PRC government can act on the vulnerability for its own purposes before network defenders can be made aware of a risk.

In the Board's judgment, Alibaba's researcher acted responsibly by following a sound coordinated disclosure process with ASF, and the Board is concerned about alleged punitive government sanctions creating a chilling effect on future coordinated disclosure.

Information Overload

Numerous interviewees highlighted the overall unity of effort and communications across the broader cyber community, noting a sense of common struggle against an unprecedented and dangerous new vulnerability. They also observed that the flood of well-intentioned information soon became overwhelming, rather than empowering, for impacted organizations. This was especially true during the initial response, due to the amount of information coming from security researchers on Twitter,[139, 140] notifications from ASF, vendor security alerts, press coverage, and notifications from government agencies, such as CISA. In a sea of alerts about potential mitigations and defensive measures, network defenders sought authoritative guidance that they could confidently take to their teams and execute against.[141] Appendix D provides more insight into the amount of information that inundated responders.

The impact of this information overload is apparent in the sequence of multiple releases of Log4j upgrades as researchers discovered additional security flaws (see Section 1.2 – Discovery and Disclosure). Due to continuous releases of upgrades, organizations had to consume new information in real time in order to understand to which version they should upgrade relative to their overall risk posture. Some turned to CVSS scores for insights into their risk exposure. However, CVSS scores do not provide insight into the impact of the vulnerability in the context of an organization's business assets, exposure, or operations, or the specific intent of attackers exploiting the vulnerability. As impacted organizations attempted to prioritize these risks and determine remediations, they were forced to sort through bulletins, advisories, and guidance from vendors, media, partners, and government sources.

Organizations also faced information overload from their own security monitoring programs. After disclosure of the vulnerability, organizations reported observing widespread vulnerability scanning, and many were unable to distinguish attackers from bona fide researchers. This meant organizations found it challenging to understand whether or not malicious threat actors were attacking their systems. Some organizations offered resources to help focus responders, for example GreyNoise has a free community portal to help identify known malicious and known benign (including research) scans.[142]

2.5 IMPACT ON BUSINESS OPERATIONS

Given the scale of use of Log4j, the ease of exploiting the vulnerable feature, and widespread reporting on the vulnerability, the Board expected to find during its review that the vulnerability had a significant impact on the safety of the digital ecosystem. However, at the time the Board concluded its review, despite industry

[139] Chief executive; Cybersecurity technology services company. Subcommittee Meeting.
[140] Recent vulnerability management efforts indicate heightened involvement of non-traditional and informal partnerships. Throughout the Log4j and SolarWinds events, researchers and defenders used social media as a primary communication vehicle to exchange emergent information in real time. *Source: Cybersecurity and Infrastructure Security Agency (CISA). Response to Board request for information. May 6, 2022.*
[141] Chief executive; Non-profit organization. Subcommittee Meeting.
[142] The GreyNoise Team, "GreyNoise Community," https://www.greynoise.io/plans/community

observations of widespread exploitation attempts (see Section 1.3 – Exploitation), the Board did not learn of any significant attacks impacting organizations, including attacks on critical infrastructure.[143]

Several factors provide context for this outcome. First, while cybersecurity vendors could provide anecdotal evidence of exploitation, the Board found it challenging to identify an authoritative source from which to understand exploitation trends across geographies, industries, or ecosystems. Many organizations did not collect or report information on specific Log4j exploitation. The use of scanning techniques that limited the ability to differentiate between benign and malicious activity during the Log4j event further complicated this picture. Second, information about which organizations were impacted, and specific threat activity (for example advanced persistent threats (APTs)), is generally limited to information that victims voluntarily report. No central repository of information about Log4j-related breaches exists, and mandatory reporting requirements that would make one possible are limited or not yet in legal effect.

However, many organizations did report to the Board that they saw a negative impact to their business operations due to the complex nature of Log4j response efforts, which required them to reallocate significant resources in a short period of time. For example, one federal cabinet department reported dedicating 33,000 hours to Log4j vulnerability response.[144] These responses, often sustained over many weeks and months, resulted in high costs and delayed other mission-critical work, including responding to other vulnerabilities.

In the long term, the collective need for crisis-driven risk management distracts resources and management attention from foundational investments that would support rapid response in future incidents. In the case of the Log4j event, for example, the forced speed of response and challenges of managing risk induced professional "burnout" among defenders that could have a long-term impact on cybersecurity talent attrition.[145] Cybersecurity professionals cannot collectively sustain a model where most of their resources are spent reacting to emerging problems like a steady stream of vulnerabilities.

At this time, Log4j has become an "endemic vulnerability" that will be exploited for years to come.[146, 147] The impact to organizations over the long term will be difficult to assess without better tools for discerning real exploitation and centralized reporting of successful compromises.[148]

---

[143] In an adjacent process, at the request of the Board, the U.S. intelligence community provided a summary that its own analysis does not contradict the factual information captured in the Board's facts and findings, pertaining to the Logj4 vulnerability timeline, exploitation, and impact to U.S. interests.
[144] Federal Chief Information Security Officer (CISO). Subcommittee Meeting.
[145] David C., U.K National Cyber Security Centre (NCSC-UK), December 17, 2021, "Log4j vulnerability: what should boards be asking?" December 17, 2021, https://www.ncsc.gov.uk/blog-post/log4j-vulnerability-what-should-boards-be-asking
[146] Federal Chief Information Security Officer (CISO). Subcommittee Meeting.
[147] Technology services company. Response to Board request for information.
[148] The SolarWinds event also demonstrated the need for organizations to manage risk over the long-term: threat actors had access to SolarWinds' systems for approximately 14 months. They also deployed malware designed to remain dormant for 14 days before executing code. *Source: Mandiant (FireEye), "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor," December 13, 2020, https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor*

SECTION 3 – RECOMMENDATIONS

The recommendations outlined in this section respond to the Board's mandate to identify improvements for cybersecurity and make independent, strategic, and actionable recommendations to the Secretary of Homeland Security, while recognizing that the Log4j event is ongoing and the vulnerability continues to potentially expose organizations. The Board notes that the community should implement improvements to forestall the next Log4j-type event while also undertaking actions to intervene and remediate the present risks. Therefore, our recommendations blend the need for continued vigilance with a drive toward medium-term adoption of existing security hygiene best practices and investments to improve cybersecurity processes, frameworks, and policies. Additionally, new investment and novel approaches are necessary to bring about transformations that scale to protect the entire the ecosystem at an optimal level of capability and maturity.

The Log4j event occurred amid a wider conversation to improve the nation's cybersecurity posture, where private and public sector partnerships are developing promising new policy and industry-led actions such as the shift to Zero Trust architectures, new strategies for software assurance, and new requirements for reporting incidents. Many of these efforts were still nascent at the time of this report's production, but merit special acknowledgement in their respective contexts as they relate to the Log4j event. Where applicable, we have recognized where those efforts are related to the Board's recommendations.

The Board's recommendations are organized under four themes:

1. **Address Continued Risks of Log4j**: promote continued vigilance in addressing Log4j vulnerabilities for the long term;
2. **Drive Existing Best Practices for Security Hygiene**: adopt industry-accepted practices and standards for vulnerability management and security hygiene;
3. **Build a Better Software Ecosystem:** drive a transformation in the software ecosystem to move to a proactive model of vulnerability management; and
4. **Investments in the Future**: research possible cultural and technology shifts necessary to solve for the nation's digital security.

ADDRESS CONTINUED RISKS OF LOG4J

The Board predicts that, given the ubiquity of Log4j, vulnerable versions will remain in systems for the next decade, and we will see exploitation evolve to effectively take advantage of the weaknesses.

1. Organizations should be prepared to address Log4j vulnerabilities for years to come.

All organizations should have capabilities to discover and upgrade vulnerable software and the ability to sustain execution of these vulnerability management capabilities for the long term.

- All organizations should continue to proactively monitor for and upgrade vulnerable versions of Log4j.
- All organizations should prioritize applying software upgrades (using mitigations sparingly) as described in Section 2.4 – Ecosystem Risk Management, to avoid errant conditions that would create exposure over the long term (for example, configuration mistakes that expose vulnerable attack surfaces).
- All organizations should use robust business processes that prevent the reintroduction of vulnerable versions of Log4j (regressions).
- All organizations should take a risk-based approach to remediating Log4j so they can address other high-severity vulnerabilities.

2. Organizations should continue to report (and escalate) observations of Log4j exploitation.

Maintaining collective defense against the ongoing Log4j exploitation requires all stakeholders to share insights about activity they are observing.

- Federal agency Chief Information Security Officers (CISOs) should report instances of Log4j exploitation to CISA even if they do not meet the threshold for a significant event.
- All organizations are encouraged to report significant incidents resulting from Log4j exploitation to the FBI or CISA.
- CISA should expedite, to the greatest extent possible, its implementation of the landmark cyber incident reporting requirements Congress enacted in March 2022 through the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).[149] The new mandate requires CISA to conduct initial rulemaking activities within 24 months, but CISA should conduct its implementation as quickly as possible within that timeframe.
- The Cyber Incident Reporting Council[150] should prioritize recommendations that will ensure that significant exploitations of vulnerabilities like Log4j are promptly reported to CISA and other appropriate agencies.

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 contains elements designed to increase observation of vulnerability exploitation. For example, CIRCIA:

- establishes a requirement for critical infrastructure entities to report cyber incidents within 72 hours of discovery;
- protects proprietary information from misuse;
- shields reporting entities from liability as a result of the reporting; and
- creates the Cyber Incident Reporting Council, chaired by the Department of Homeland Security, to review and recommend actions to harmonize cyber incident reporting requirements across federal regulatory, law enforcement, and sector risk management agencies.

3. CISA should expand its capability to develop, coordinate, and publish authoritative cyber risk information.

Many organizations faced challenges in identifying authoritative sources of information to effectively respond to the Log4j vulnerability. CISA, as the operational lead for federal cybersecurity and national coordinator for critical infrastructure security and resilience, is the natural federal lead to collect and disseminate authoritative information before, during, and after a cyber event.

- CISA should continue to evaluate Log4j exploitation risk and enhance the risk management capabilities of the broader community through interagency coordination. To achieve this objective:
    - the Intelligence Community should provide to CISA ongoing assessments of the capability and intent of threat actors to exploit the Log4j vulnerability;
    - federal CISOs and the JCDC should provide to CISA those vulnerabilities that, if exploited, would yield significant impact to critical infrastructure, national security, or the economy; and

[149] H.R.2471 - 117th Congress (2021-2022): Consolidated Appropriations Act, 2022, "Cyber Incident Reporting for Critical Infrastructure Act of 2022," https://www.congress.gov/bill/117th-congress/house-bill/2471/text

[150] Congress, through CIRCIA, created a new multi-agency Cyber Incident Reporting Council, which the Department of Homeland Security will chair, to review and recommend actions to harmonize cyber incident reporting requirements across federal regulatory, law enforcement, and sector risk management agencies.

  - CISA should solicit, analyze, and integrate non-federal and federal data, including threat, consequence, and vulnerability data, to yield actionable information to enhance Log4j risk management.

- CISA should enhance communication by designating resources to widely distribute actionable information to stakeholders and continue to invest in trusted relationships to prepare for the next incident. CISA should continue to:
  - validate information sources and coordinate authoritative messaging during ongoing significant cybersecurity events;
  - leverage existing trust communities such as Information Sharing and Analysis Organizations (ISAOs) and Information Sharing and Analysis Centers (ISACs), and public-private sector partnerships; and
  - methodically expand industry partner relationships with organizations that can provide telemetry data, exploitation trends, and insight into ongoing threat actor activity to obtain a more informed understanding surrounding cybersecurity incidents, promote optimized information sharing mechanisms, and enable reliable and constructive response efforts across varying event types.
- CISA should request that members of the JCDC periodically measure Log4j exploitation and determine whether and where (for example, by industry, sector, or platform) alerts and advisories could help reinforce the need for patching and mitigation.
- CISA, in coordination with the FBI and the Intelligence Community, should develop a joint cyber threat model for projecting advanced adversaries' long-term exploitation capabilities based on their historical TTPs.

4. Federal and state regulators should drive implementation of CISA guidance through their own regulatory authorities.

CISA operates on a voluntary cooperation model with industry, but regulators have the legal authorities to drive better cybersecurity by compelling or encouraging their regulated communities to comply with CISA's guidance. The FTC showed leadership in this respect by pointing its stakeholders to CISA's Log4j guidance, following CISA's engagement with the FTC to educate the agency about the vulnerability and effective mitigations.

- Federal and state regulators across industry sectors should identify opportunities to direct or encourage their regulated communities to implement CISA guidance, advisories, and best practices. DHS, and specifically CISA, should similarly encourage federal and state regulators to become familiar with CISA's products and offer those regulators support in amplifying them.

DRIVE EXISTING BEST PRACTICES FOR SECURITY HYGIENE

Organizations should adopt current industry-accepted practices and standards for vulnerability management and security hygiene.

5. Organizations should invest in capabilities to identify vulnerable systems.

Organizations should invest in capabilities that allow them to identify vulnerable systems and applications in their environments in a timely manner.

- All organizations, including U.S. government agencies, should maintain an accurate asset and application inventory (as discussed in Recommendation 6), using automation and tooling as

necessary, as outlined in International Organization for Standardization (ISO) 55000:2014[151] and NIST Special Publication 1800-5.[152]

- Organizations should deploy vulnerability scanning technologies that will identify vulnerable software in line with recommendations from ISO 27001:2018.[153]
- As vulnerability identification capabilities mature (see Recommendation 12 on SBOMs), organizations should be prepared to champion and adopt new technologies to enhance the speed of vulnerability mitigation.

The Open Source Software Security Mobilization Plan,[154] led by the Linux Foundation and Open Source Security Foundation (OpenSSF), calls for industry action to develop software component frameworks (including SBOMs) to expedite discovery of and response to future vulnerabilities like Log4j.

6. Develop the capacity to maintain an accurate IT asset and application inventory.

Maintaining an accurate technology asset and application inventory is an accepted industry-wide best practice of cyber hygiene, and can help organizations more easily identify affected assets and applications in responding to an incident. All organizations should maintain an accurate IT asset and application inventory, and the Board recommends that within the U.S. government:

- the Office of Management and Budget (OMB) should take appropriate steps to ensure that federal agencies invest in automation and tooling to establish and maintain an accurate and robust technology asset and application inventory;
- CISA should coordinate with federal agencies to map direct and indirect software dependencies across open and commercial software throughout the federal enterprise to improve detection and incident response when vulnerabilities are found in software dependencies; and
- OMB, in coordination with the Office of the National Cyber Director (ONCD) and CISA, should, as the SBOM ecosystem matures, consider issuing guidance to agencies on effectively using these asset inventories and software metadata to improve detection and incident response during future vulnerability response activities.

7. Organizations should have a documented vulnerability response program.

Vulnerability response is the process of investigating a potential security incident or emerging cyber threat to take defensive or corrective action. It refers to remediating both publicly-known vulnerabilities as well as active attacks that are under private investigation. This process differs from vulnerability disclosure and handling processes in that it deals with vulnerabilities affecting the software that organization uses but for which it is not the code maintainer.

---

[151] International Organization for Standardization (ISO), "ISO 55000:2014: Asset management — Overview, principles and terminology," July 2014, https://www.iso.org/standard/55088.html
[152] National Institute of Standards and Technology (NIST), "SP 1800-5: IT Asset Management," September 2018, https://csrc.nist.gov/publications/detail/sp/1800-5/final
[153] International Organization for Standardization (ISO), "ISO/IEC 27000:2018: Information technology — Security techniques — Information security management systems — Overview and vocabulary," February 2018, https://www.iso.org/standard/73906.html
[154] Open Source Security Foundation (OpenSSF), "*The Open Source Software Security Mobilization Plan*," https://openssf.org/oss-security-mobilization-plan/

- Organizations that consume software, including U.S. government agencies, should have a documented vulnerability response program as described in Cybersecurity Incident & Vulnerability Response Playbooks[155] and ISO/IEC 27001:2018.[156]
- Organizations should holistically assess, aggregate, classify, and prioritize high-risk vulnerabilities for software running on their systems.
- Organizations should increase the maturity of their vulnerability response program, especially where they currently have limited capabilities, by setting benchmarks and measuring their efficacy over time.

8. Organizations should have a documented vulnerability disclosure and handling process.

Vulnerability disclosure and handling are the processes that define how organizations should receive and process vulnerability reports in products or systems for which they are responsible for creating the fix. The vulnerabilities handled in this set of processes could be in code the organization wrote or maintains, or they could be in erroneous configurations or outdated systems the organization owns.

- Organizations, including open source projects, should assume that publicly visible code changes, code comments, and release candidates containing security vulnerability fixes are equivalent to public disclosure of such issues. Organizations should have plans to release security advisories concurrently, including for any public code commits or mitigations to address security vulnerabilities.
- Organizations should prepare to receive vulnerability reports and act on them to investigate, prioritize, and create remediations.[157]
- Organizations should make investments in software supply chain security, such as securing their Continuous Integration/Continuous Delivery (CI/CD) pipeline and establishing vulnerability coordination communication channels with supply chain partners to facilitate smoother and more efficient vulnerability coordination.
- Organizations should measure their mean time to repair (MTTR) vulnerabilities that are reported to them to ensure they are able to investigate and resolve vulnerabilities in code they maintain or deploy in a timely manner.

Software developers and maintainers should be prepared to participate in vulnerability handling and coordinated vulnerability disclosure, including participation in relevant multi-party supply chain vulnerability coordination, per guidance in ISO 29147:2018[158] and ISO 30111:2019.[159] To support organizations in their work to develop vulnerability disclosure and handling process:

- CISA should continue to encourage and, where possible, incentivize parties that discover vulnerabilities (for example security researchers or outside developers), to disclose them to the affected vendor or a trusted third party.

---

[155] Cybersecurity and Infrastructure Security Agency (CISA), "Cybersecurity Incident & Vulnerability Response Playbooks: Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems," November 2021, https://cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

[156] International Organization for Standardization (ISO), "ISO/IEC 27000:2018: Information technology — Security techniques — Information security management systems — Overview and vocabulary," February 2018, https://www.iso.org/standard/73906.html

[157] International Organization for Standardization (ISO), "ISO/IEC 29147:2018: Information technology — Security techniques — Vulnerability disclosure," October 2018, https://www.iso.org/standard/72311.html

[158] International Organization for Standardization (ISO), "ISO/IEC 29147:2018: Information technology — Security techniques — Vulnerability disclosure," October 2018, https://www.iso.org/standard/72311.html

[159] International Organization for Standardization (ISO), "ISO/IEC 30111:2019: Information technology — Security techniques — Vulnerability handling processes," October 2019, https://www.iso.org/standard/69725.html

- Computer Emergency Response Team Coordination Center (CERT/CC) should be given additional personnel and other resources to facilitate increasing its current coordination capacity in anticipation of increased ecosystem-wide software supply chain vulnerability coordination events.

9. Software developers and maintainers should implement secure software practices.

Software developers and maintainers should adopt standard practices and technologies to build secure software in accordance with ISO 27034:2011[160] and NIST's Secure Software Development Framework.[161]

- Software developers and maintainers should establish a comprehensive approach to code maintenance that encompasses consistent secure development processes, and accounts for software security assessments and vulnerability management operations, as well as patch creation and coordinated disclosure.
- To minimize inadvertent risk, as a best practice, code maintainers should implement communication processes and mechanisms that provide consistent and relevant security messaging to software package users, noting all recommended data to include in a security advisory.
- Software developers and maintainers should leverage Integrated Development Environment (IDE) tools and add-ons for assisting in secure software development, consistent with NIST's Secure Software Development Framework.[162]
- Software developers and maintainers should also integrate source code scanning and tools that provide software maintenance status and versions to heighten their situational awareness of applications and software used within the environment.

BUILD A BETTER SOFTWARE ECOSYSTEM

The Log4j incident highlighted the need to evolve industry-accepted practices and technologies that lead to software that is secure by design.

10. Open source software developers should participate in community-based security initiatives.

Given the wealth of resources now available for the development of secure open source software, developers should engage in security uplift programs. The Board recognizes organizations should select the best programming options for their needs, so the Board lists some options below for reference only.

- OpenSSF offers the following resources to the open source community: security training and community resources;[163] auditing services through the Alpha Omega initiative to optimize security without increasing overhead;[164] and security Scorecards,[165] which allow a project to assess its risk and security posture.

---

[160] International Organization for Standardization (ISO), "ISO/IEC 27034-1:2011: Information technology — Security techniques — Application security — Part 1: Overview and concepts," November 2011, https://www.iso.org/standard/44378.html
[161] National Institute of Standards and Technology (NIST), "SP 800-218 - Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities," February 2022, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf
[162] National Institute of Standards and Technology (NIST), "SP 800-218 - Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities," February 2022, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf
[163] Open Source Security Foundation (OpenSSF), "Secure Software Development Fundamentals Courses," https://openssf.org/training/courses/
[164] Linux Foundation (LF)/Open Source Software Foundation (OpenSSF). Board Meeting.
[165] OpenSSF, GitHub, "Security Scorecards," https://github.com/ossf/scorecard

- Open Web Application Security Program (OWASP) Foundation,[166] which tracks community-led open source projects and focuses on improving the security of software, offers publicly available data tracking the top security risks to web applications, as well as tools and resources for developers, including education, training, and community networking.
- *The Open Source Software Security Mobilization Plan* has several workstreams focused on assisting the open source community through heightened security for critical components, including code audits, and improving the software development and build process.[167]

11. Invest in training software developers in secure software development.

Software developers come from a range of backgrounds and often do not have access to formal training programs. Furthermore, students earning accredited computer science degrees or other types of certifications generally have no requirement to conduct hands-on study of secure coding practices, nor is knowledge of secure programming required for building software.

- The U.S. government should continue to invest in and engage with higher education institutions and training programs by:
    - establishing and incentivizing cybersecurity curricula and certification programs, and integrating cybersecurity modules into all computer science programs, similar to the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program (managed by NSA, with multiple federal partners) and NIST's cybersecurity education initiatives;[168]
    - determining a strategic approach on how to influence educational initiatives as a component of a national cyber education strategy, such that recommended security training is integrated into requirements for computer science degrees and IT certifications. Congress should consider amendments to the Bipartisan Innovation and Competition Act to this effect (Numerous precedents exist for more active federal involvement in educational matters with security implications, such as the National Research Act of 1974); and
    - ONCD should develop a strategic engagement strategy in collaboration with the National Governor's Association, the Education Commission of the United States, and leading educational organizations (e.g., ABET, CSAB, AAUP, APLU, ACE, AAU, and HLC[169]) to implement the above recommendations. The strategy should include recommendations for a national cyber education strategy that incentivizes including security training into requirements for computer science degrees and IT certifications.
- Universities and community colleges should incorporate cybersecurity training and secure development practices as required components of computer science programming degrees and certifications.
    - Accredited computer science degrees should provide training in secure coding practices and cybersecurity fundamentals.

---

[166] Open Web Application Security Program (OWASP) Foundation, "*About the OWASP Foundation*," https://owasp.org/about/
[167] Open Source Security Foundation (OpenSSF), "*The Open Source Software Security Mobilization Plan*," https://openssf.org/oss-security-mobilization-plan/
[168] Central Security Service, National Security Agency (NSA), "National Centers for Academic Excellence in Cybersecurity," https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/
[169] AAUP is the American Association of University Professors; APLU is Association of Public Land Grant Universities; ACE is the American Council on Education; HLC is the Higher Learning Commission; ABET is Accreditation Board for Engineering and Technology; CSAB is Computer Sciences Accreditation Board; and AAU is Association of American Universities.

The Open Source Software Security Mobilization Plan includes a goal to secure open source software by delivering baseline secure software development education and certification to all.[170]

12. Improve SBOM tooling and adoptability.

Organizations need the ability to quickly identify vulnerable software to facilitate swift response. Traceability capabilities, such as SBOMs that can catalog the components of software, are promising possibilities, but at present are limited. The Board anticipates future improvements in SBOM implementations and adoption, which may enable organizations to leverage SBOMs for vulnerability management. In the meantime, the Board recommends that:

- software developers should generate and ship SBOMs with their software, and be prepared to incorporate improvements in the tooling and processes as they become available to the industry.

Executive Order (EO) 14028 *Improving the Nation's Cybersecurity* provides a roadmap for the inclusion of SBOMs when providing software to the federal government.[171]

The Board also lends its support to efforts, such as *The Open Source Software Security Mobilization Plan*, that advocate for SBOM improvements to create friction-free seamless tooling and training, and drive adoption industry-wide.[172]

13. Increase investments in open source software security.

The U.S. government is a significant consumer and producer of open source software, and therefore should play a role in driving security enhancements to the overall open source ecosystem.

- OMB should take appropriate steps to direct federal agency IT staff to contribute to the security and maintenance of open source software upon which they rely, as part of their regular duties.
- ONCD, in coordination with OMB, should consider effective funding mechanisms to invest in widely used open source software tools, and to catalyze improvements in the overall security of the open source software ecosystem.
- NIST should engage with the open source software community to develop practical guidance on how to most effectively apply federal policies and frameworks around secure software development for open source software.

Private sector companies that build commercial software that includes open source libraries or dependencies should commit financial resources toward the open source projects that they deploy. Specific examples include:

- paying developers, security engineers, and other essential roles in supporting secure software development, vulnerability disclosure and handling processes, and vulnerability response for open source projects; and
- contributing funding and knowledge to centralized open source security projects.

---

[170] Open Source Security Foundation (OpenSSF), "*The Open Source Software Security Mobilization Plan*," https://openssf.org/oss-security-mobilization-plan/
[171] Executive Order (EO) 14028, "*Improving the Nation's Cybersecurity*," May 12, 2021, https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity
[172] Open Source Security Foundation (OpenSSF), "*The Open Source Software Security Mobilization Plan*," https://openssf.org/oss-security-mobilization-plan/

The White House Meeting on Software Security (2022) called for software maintainers to invest in the regular maintenance of open source software.[173]

14. Pilot open source software maintenance support for critical services.

The Board heard from many interviewees about the operational risks introduced to organizations because of limitations in open source software maintenance. Open source developers are usually not paid to maintain their software, especially not older versions that are often deployed deeply and widely across systems. Log4j was a particularly extreme example of this. The burden of maintenance then falls to organizations that use open source software, and can be expensive, time-consuming, and unpredictable. Organizations should be able to project the maintenance costs of open source software, and obtain that information from a trusted source. Funding the maintenance of critical open source software could drive a more sustainable model for security at scale and enable timely and effective distribution of updates and mitigations.

A collaborative organization, such as Critical Infrastructure Partnership Advisory Council (CIPAC), should work with the Forum of Incident Response and Security Teams (FIRST) to bring the membership of major vendors' Product Security Incident Response Teams (PSIRTs) together with both public and private sector partners (including OpenSSF) to pilot a collection of the most commonly included open source libraries or dependencies that would:

- generate a critical open source package list for major industries, leveraging the PSIRTs' data and criteria such as OpenSSF's Criticality Score;
- project the costs associated with managing the collection and identify funding streams from government and private sector;
- develop and apply a framework for maintenance of packages, including protocols that are automated where possible, to dynamically swap out old and vulnerable libraries; and
- establish security requirements and associated metrics for tracking and reporting (in tandem, this could leverage OpenSSF's Scorecard project and similar endeavors).

INVESTMENTS IN THE FUTURE

To address the significant challenges present in the current software ecosystem, innovative solutions will be necessary. The Board proposes several areas for additional examination and research towards this goal.

15. Explore a baseline requirement for software transparency for federal government vendors.

The U.S. government is a significant consumer of software, and should be a driver of change in the marketplace around requirements for software transparency.

- OMB and the Federal Acquisition Regulatory (FAR) Council should use various mechanisms to minimize the U.S. government's use of software without provenance and dependency information, and should consider the use of procurement requirements, federal standards and guidelines, and investments in automation and tooling, to create clear and achievable expectations for baseline SBOM information.
- OMB should set a specific timeframe to achieve these goals.

[173] The White House, "Readout of White House Meeting on Software Security," January 13, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/

16. Examine the efficacy of a Cyber Safety Reporting System (CSRS).

The U.S. government, via NIST in conjunction with CISA, should convene a public-private working group to examine the risks, efficacy, and requirements for a potential U.S. government-run Cyber Safety Reporting System (CSRS). Similar to the National Aeronautics and Space Administration's (NASA's) Aviation Safety Reporting System, a CSRS could contribute to a system-wide view of the cyber ecosystem and expand and centralize the existing external reporting and coordination of cyber safety issues.

Built on a voluntary model, a CSRS could incentivize anonymized reporting of exploitable vulnerabilities in key libraries, software code bases, and key projects. Principles central to operation of such a system include:

- weighing how to anonymize reporting of vulnerabilities and safety defects;
- how to incentivize reporting and protocols as non-punitive; and
- determining independence and non-regulatory use of the system.

This type of system could also support federally-coordinated efforts to prioritize the identification, monitoring, and remediation of software issues that might affect National Critical Functions—supporting systemic risk coordination and identifying where common safety issues exist in complex operating environments across multiple organizations, such as supply and operating chains.

As part of this examination, the working group should consider the risks associated with aggregation of vulnerabilities and reliance on voluntary reporting of data. This working group should also consider:

- workflow of government and industry information reported via the CSRS;
- scalability and effectiveness;
- public transparency and accountability; and
- composition of any oversight function.

Lastly, the working group should aim to complete its work and make any substantive recommendations within a six-month period following its establishment.

17. Explore the feasibility of establishing a Software Security Risk Assessment Center of Excellence (SSRACE).

There is no centralized inventory of open source and proprietary software across federal agencies. CISA should explore the feasibility of creating, in collaboration with the private sector, a Software Security Risk Assessment Center of Excellence (SSRACE) to develop, manage, and protect a central inventory of all software across federal agencies. Such an inventory would facilitate effective notification of and response to software vulnerabilities; enhance capability for risk management; and serve as a source of data to inform systemic-level risk assessment and drive priority of security improvement.

In parallel, the SSRACE should also advance the following efforts:

- identify the open source software used by the U.S. government to support critical mission delivery, and advocate for funding from U.S. government grants and commercial sponsorship to support open source software foundations to improve software safety;
- establish principles, metrics, and transparency to drive prioritization and assess improvement;
- develop performance requirements for industry-wide standard support functions vital to the rapid operational risk assessment of vulnerable software. Advocate for existing standards (e.g., CVE, Common Platform Enumeration (CPE), Common Configuration Enumeration (CCE)), or champion the creation and use of new industry standards. Examples include standard naming of vulnerabilities, software versions, development metadata; and

- identify and advocate for best practices in lifecycle management and incentives for vendors to use code that can support timely software updates and mitigations for critical vulnerabilities.

18. Study the incentive structures required to build secure software.

Many interviewees stressed the volunteer nature of the open source software community. In light of that, the Board recommends the U.S. government's National Academy of Sciences Cyber Resilience Forum undertake a study of incentive structures to build secure software. The Forum should consider:

- legal, structural, and regulatory incentives for organizations, to include, for example, the potential for software liability reform;
- developer incentive structures that increase awareness of safety issues. For example, developers could obtain a trust rating for their contributions through extended education on secure coding or threat modeling. This developer rating could be a component of the software's overall health rating; and
- challenges to adopting incentives, including, but not limited to, resourcing and volunteer fatigue.

The Open Source Software Security Mobilization Plan proposes initial ideas to incentivize the adoption of secure software practices such as training and badges.[174]

19. Establish a government-coordinated working group to improve identification of software with known vulnerabilities.

Recognizing that the industry faces challenges with current approaches to vulnerability identification and mitigation, NIST should convene a working group, to include private sector expertise, to determine if and how better methods can be developed.

- This effort should include the National Science Foundation (NSF), given its vantage point into possible academic research that exists in this area.

The working group should explore if software can become self-managed, or even self-aware, at a level of capability where software reports, if not takes actions, based on self-identification of known vulnerabilities. The outcome of the working group should be to try to create a standard that industry can adopt—to disrupt the traditional vulnerability discovery and software maintenance process, which currently relies on imperfect and incomplete scanning methods for vulnerable systems and software.

- The working group should conclude its work within three years.

[174] Open Source Security Foundation (OpenSSF), "*The Open Source Software Security Mobilization Plan*," https://openssf.org/oss-security-mobilization-plan/

APPENDIX A: CSRB PRINCIPLES

At its inaugural meeting on February 25, 2022, the Cyber Safety Review Board voted that it will conduct its work consistent with the following principles.

- Public service. The Board will act in the public interest and will operate with integrity. Members will offer expertise and independent judgment for the benefit of the Board and the nation's cybersecurity.
- Transparency and trust. The Board will share public versions of its reports to build trust through transparency. The Board will protect sensitive information it receives consistent with applicable law.
- Objective, forward-looking reviews. The Board will utilize its fact-finding mission to facilitate lessons learned and advance the cybersecurity goals of the United States. The Board is not a regulatory body and is not focused on finger-pointing. It will foster a just culture and focus on formulating actionable, realistic, and timely recommendations to better secure the community.
- Diversity advances outcomes. Diverse perspectives and professional backgrounds enrich analysis and outcomes and will be aggressively sought in the review process.
- Focus on impact. The Board will focus on formulating recommendations that are actionable, realistic, and timely.
- Pursue solutions to root causes. The Board will be ambitious about recommending both novel and proven solutions that address root causes in the near, medium, and long term.
- Expertise matters. The Board will source the highest quality data and expert analysis available.
- Celebrate success. The Board will propel best practices through the recognition and promotion of identified successes, so that positive lessons learned can be translated into community-wide momentum.

APPENDIX B: SUMMARY OF CSRB INTERVIEWS AND REQUESTS FOR INFORMATION

Through the course of the CSRB's review and in addition to its review of publicly available material, the CSRB met with representatives from nearly 40 separate organizations and requested information from 60 organizations comprised of developers, end users, and defenders. These organizations included:

- cloud and mobile services providers;
- critical infrastructure operators and maintainers;
- cybersecurity service providers and researchers;
- foreign government cybersecurity organizations;
- open source software foundations and developers;
- product developers; and
- U.S. government agencies and departments.

A complete list of companies engaged during the Log4j review is provided below. The Board officially contacted these companies to either voluntarily provide data and/or meet with the Board to provide commentary of the Log4j event from their organization's perspective. Though this list is comprehensive, the Board recognizes that it could have contacted additional organizations if given additional time to conduct interviews and submit requests for information.

1 – Request for information submitted and received (in whole or in part)
2 – Interviewed by the Board
3 – Interviewed by Staff
4 – No response or declined to respond
5 – Information proactively provided to the Board

Organization

Akamai Technologies, Inc.[1, 3]

Alibaba Group Holding Limited[1]

Amazon Web Services, Inc.[2]

Apache Software Foundation, The[1,2]

Apple Inc.[4]

Arctic Wolf Networks, Inc.[1,3]

AT&T Inc.[1]

Atlantic Council of The United States Inc.[1,3]

BigFix, Inc.[2]

Boeing Company, The[2]

BoundaryX[4]

CERT Division, Software Engineering Institute, Carnegie Mellon University[2]

Cisco Systems, Inc.[1,2]

Cisco Talos[1]

Citigroup Inc.[2]

Cloudflare, Inc.[1,2]

CrowdStrike, Inc.[1,2]

Cybersecurity and Infrastructure Security Agency[1,2]

Dragos, Inc.[2]

Google LLC[1,2]

GreyNoise Intelligence, Inc.[1,2]

Kaiser Foundation Hospitals Inc.[4]

Mandiant, Inc.[1,2]

Microsoft Corporation[1,2]

MobileIron, Inc.[1]

Israel National Cyber Directorate[2]

National Railroad Passenger Corporation (dba Amtrak)[2]

Open Information Security Foundation Inc.[2]

Open Source Developer Panel[2]

Open Source Security Foundation, The Linux Foundation[2]

Oracle Corporation[1,2]

Palo Alto Networks Inc.[4]

PRC Ministry of Industry and Information Technology
(submitted via the PRC Ambassador to the United States)[1]

Rapid7, Inc.[2]

Recorded Future, Inc.[1]

Ring Protect Inc.[4]

SecureWorks Corporation[1]

Shostack & Associates Inc.[2]

Software Bill of Materials (SBOM) Expert Panel[2]

Sonatype, Inc.[4]

Synopsys, Inc.[1,3]

Tenable, Inc.[2]

Trellix[1,3]

Thermo Fisher Scientific Inc.[4]

Ubiquiti Inc.[4]

U.K. National Cyber Security Centre[2]

United States Agency for International Development[1,3]

United States Department of Agriculture[1]

United States Department of Commerce[1]

United States Department of Defense[1]

United States Department of Education[1,2,3]

United States Department of Energy[1]

United States Department of Health and Human Services[1]

United States Department of Homeland Security[3]

United States Department of Housing and Urban Development[1]

United States Department of Interior[1]

United States Department of Justice[1]

United States Department of Labor[1]

United States Department of State[1]

United States Department of Transportation[1]

United States Department of Treasury[3]

United States Environmental Protection Agency[1]

United States General Services Administration[1]

United States National Aeronautics and Space Administration[2]

United States National Cyber-Forensics and Training Alliance[2]

United States National Science Foundation[1]

United States National Telecommunications and Information Administration[1]

United States Nuclear Regulatory Commission[1]

United States Office of Management and Budget[1]

United States Office of Personnel Management[3]

United States Patent and Trademark Office[2]

United States Small Business Administration[1]

United States Social Security Administration[1]

United States Veterans Affairs[1]

Verizon Communications Inc.[1]

VMware, Inc.[4]

Wiz Cloud LTD | Ernst & Young Infrastructure Advisors, LLC[5]

ZeroFox, Inc.[1]

APPENDIX C: PRECURSORS TO CVE-2021-44228 DISCOVERY

This section provides context on Log4j's development and deployment and examines several notable events preceding the discovery of CVE-2021-44228.

Log4j deployment increased significantly in the years following its release and grew in popularity, becoming the 252nd most popular component by download, with 28.6 million downloads in a three-month period between August and November 2021. By December 14, 2021, almost 7,000 open source projects leveraged Log4j as a dependency.[175] The timeline in Figure 3, below, illustrates the development of Log4j from its earliest versions to later iterations.

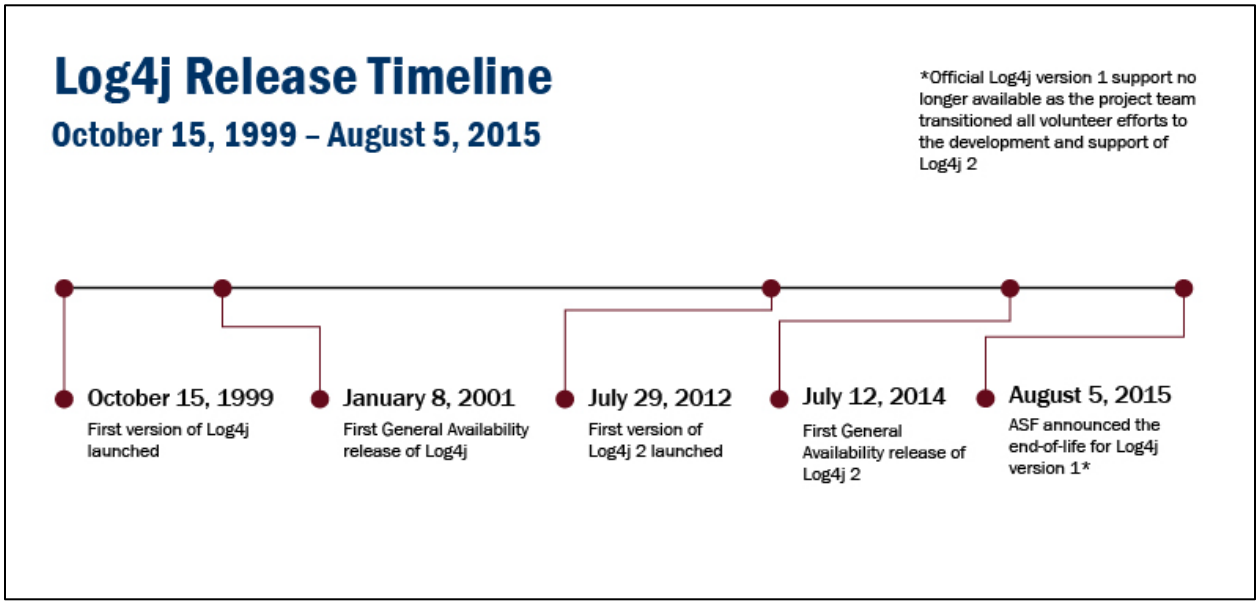

FIGURE 3 - Log4j Release Timeline

The addition of the JNDI lookup feature, first released for general availability in Log4j version 2.0 in 2014, was the pivotal modification that introduced the vulnerable attack surface for CVE-2021-44228. Before discovery and disclosure of the vulnerability, several researchers highlighted security concerns with JNDI functionality:

- a 2015 presentation illustrated the consequences of deserializing objects from untrusted data and methods to exploit these issues to achieve remote code execution;[176, 177]
- a Black Hat USA 2016 presentation demonstrated methods attackers could use to run arbitrary code by leveraging JNDI lookups;[178, 179]

[175] Turunen, Ilkka, "Log4shell by the numbers - Why did CVE-2021-44228 set the Internet on Fire?" December 14, 2021, https://blog.sonatype.com/why-did-log4shell-set-the-internet-on-fire
[176] Frohoff, Chris and Lawrence, Gabriel, AppSec California 2015, "Marshalling Pickles: How Deserializing Objects Will Ruin Your Day," January 28, 2015, https://appseccalifornia2015.sched.com/event/40c922b93ac45988f1be4da3dea27892#.VjpyL36rRhE
[177] Frohoff, Chris and Lawrence, Gabriel, OWASP Foundation (Recorded Presentation), "Marshalling Pickles – Chris Frohoff & Gabriel Lawrence – OWASP AppSec California 2015," May 7, 2015, https://www.youtube.com/watch?v=KSA7vUkXGSg
[178] Munoz, Alvaro and Mirosh, Oleksandr, Black Hat USA 2016, "A Journey from JNDI/LDAP Manipulation to Remote Execution Dream Land," August 3, 2016, https://www.blackhat.com/us-16/briefings.html#a-journey-from-jndi-ldap-manipulation-to-remote-code-execution-dream-land
[179] Munoz, Alvaro and Mirosh, Oleksandr, Hewlett Packard Enterprise (HPE), "HPE Security Fortify, Software Security Research: A Journey from JNDI/LDAP Manipulation to Remote Code Execution Dream Land," https://www.blackhat.com/docs/us-16/materials/us-16-Munoz-A-Journey-From-JNDI-LDAP-Manipulation-To-RCE-wp.pdf

- supplemental research from 2017 examined Java open source marshaling libraries and associated exploitation methods, highlighting potential attack vectors to abuse JNDI functions; and[180]
- further research in 2019 investigated an approach to trigger the deserialization of untrusted data via JNDI injection.[181]

[180] Bechler, Moritz, GitHub, "Java Unmarshaller Security: Turning Your Data into Code Execution," May 22, 2017, https://www.github.com/mbechler/marshalsec/blob/master/marshalsec.pdf
[181] Stepankin, Michael, Veracode, "Exploiting JNDI Injections in Java," January 3, 2019, https://www.veracode.com/blog/research/exploiting-jndi-injections-java

APPENDIX D: COMMUNICATIONS OVERLOAD

During the Log4j event, the community leveraged a variety of formal and informal channels alongside media communications to react and respond to the vulnerability. Many communications contained well-intentioned information, but quantity and amplification (i.e., retransmission) became overwhelming for impacted organizations. This was especially true during the initial response, when alerts, advisories, and other notifications flooded the inboxes and news feeds of defenders.

Below, the Board presents a sampling of communications to demonstrate the volume and variety of these notable data sources.

Select Communication from Developers, Government, and the Non-Profit Community

- December 10, 2021 – ASF announced the Log4j 2.15.0 release, addressing CVE-2021-44228.[182]
- December 10, 2021 – The NVD published CVE-2021-44228.[183]
- December 10, 2021 – Germany's Federal Office for Information Security (BSI) issued a warning for the Log4j vulnerability.[184]
- December 10, 2021 – NSA's Director of Cybersecurity issued an alert via Twitter noting the significant threat for Log4j vulnerability exploitation due to its widespread inclusion in software frameworks.[185]
- December 10, 2021 – CISA published an advisory calling attention to the release of Log4j Version 2.15.0.[186]
- December 11, 2021 – CISA's Director released a national statement detailing the criticality of the Log4j vulnerability.[187]
- December 12, 2021 – Switzerland's Government Computer Emergency Response Team (GovCERT) issued a warning for the Log4j vulnerability.[188]
- December 13, 2021 – CISA published a webpage and GitHub repository for the Log4j vulnerability.[189]
- December 15, 2021 – The FBI issued a public request to report exploitation.[190]

---

[182] Goers, Ralph, Apache Software Foundation (ASF), Apache PonyMail, "[ANNOUNCEMENT] Apache Log4j 2.15.0 Released," December 10, 2021, https://lists.apache.org/thread/sm5gh5m0jd7lqbbt8hs27nf28xhphbwb
[183] National Institute of Standards and Technology (NIST), National Vulnerability Database (NVD), "CVE-2021-44228 Detail," December 10, 2021, https://nvd.nist.gov/vuln/detail/CVE-2021-44228
[184] Bundesamt für Sicherheit in der Informationstechnik (BSI), Federal Office for Information Security, "Critical vulnerability in the widely used software product log4j," December 10, 2021, https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Schwachstelle_Log4j_211210.html
[185] Joyce, Rob (@NSA_CSDirector), Twitter, December 10, 2021, https://twitter.com/NSA_CSDirector/status/1469305071116636167
[186] Cybersecurity and Infrastructure Security Agency (CISA), "Apache Releases Log4j Version 2.15.0 to Address Critical RCE Vulnerability Under Exploitation," December 10, 2021, https://www.cisa.gov/uscert/ncas/current-activity/2021/12/10/apache-releases-log4j-version-2150-address-critical-rce
[187] Cybersecurity and Infrastructure Security Agency (CISA), "Statement From CISA Director Easterly On 'Log4j' Vulnerability," December 11, 2021, https://www.cisa.gov/news/2021/12/11/statement-cisa-director-easterly-Log4j-vulnerability
[188] Swiss Government Computer Emergency Response Team (GovCERT), "Zero-Day Exploit Targeting Popular Java Library Log4j," December 12, 2021, https://www.govcert.ch/blog/zero-day-exploit-targeting-popular-java-library-log4j/
[189] Cybersecurity and Infrastructure Security Agency (CISA), "CISA Creates Webpage for Apache Log4j Vulnerability CVE-2021-44228," December 13, 2021, https://www.cisa.gov/uscert/ncas/current-activity/2021/12/13/cisa-creates-webpage-apache-log4j-vulnerability-cve-2021-44228
[190] Federal Bureau of Investigation (FBI), "Seeking Victims of Log4j Vulnerability," December 15, 2021, https://www.fbi.gov/resources/victim-services/seeking-victim-information/seeking-victims-of-log4j-vulnerability

- December 15, 2021 – The European Commission, the European Union (E.U.) Agency for Cybersecurity, Computer Emergency Response Team-EU (CERT-EU), and the network of the E.U. national computer security incident response teams (CSIRTs network) released a joint statement.[191]
- December 17, 2021 CISA released ED 22-02.[192]
- December 22, 2021 – CISA, the FBI, NSA, and international security counterparts from Australia, Canada, New Zealand, and the U.K., released a joint advisory.[193]
- December 22, 2021 – NSA and the FBI issued statements on their Twitter accounts.[194, 195]
- January 24, 2022 – DoD published a memorandum, Software Development and Open Source Software, citing concerns about supply chain risk management for externally maintained code in critical DoD systems.[196]

Select Communications from the Cybersecurity Industry

Information sharing entities (e.g., ISACs and ISAOs) and cybersecurity companies leveraged social media (e.g., Twitter), blogs, webinars, and similar broadcasting methods to provide quick and comprehensive details to defenders and the wider public regarding exploitation activity.

- December 9, 2021 – Splunk issued an advisory on how to detect Log4j exploitation.[197]
- December 10, 2021 – SANS published a forum post on the Log4j vulnerability and exploitation.[198]
- December 10, 2021 – CrowdStrike published a blog post on Log4j vulnerability analysis and mitigation recommendations.[199]
- December 10, 2021 – Palo Alto issued an advisory about the Log4j vulnerability and mitigation guidance.[200]
- December 11, 2021 – Microsoft issued an advisory for preventing, detecting, and hunting for exploitation of the Log4j vulnerability.[201]

---

[191] European Union Agency for Cybersecurity (ENISA), "Joint Statement on Log4Shell," December 15, 2021, https://www.enisa.europa.eu/news/statement-on-log4shell
[192] Cybersecurity and Infrastructure Security Agency (CISA), "*Emergency Directive 22-02 Mitigate Apache Log4j Vulnerability*," December 17, 2021, https://www.cisa.gov/emergency-directive-22-02
[193] Cybersecurity and Infrastructure Security Agency (CISA), "Alert (AA21-356A): Mitigating Log4Shell and Other Log4j-Related Vulnerabilities," December 22, 2021, https://www.cisa.gov/uscert/ncas/alerts/aa21-356a
[194] National Security Agency (NSA) Cybersecurity (@NSACyber), Twitter, December 22, 2021, https://twitter.com/NSACyber/status/1473680239087824901
[195] Federal Bureau of Investigation (FBI) (@FBI), Twitter, December 22, 2021, https://twitter.com/FBI/status/1473681715730202627
[196] Department of Defense (DoD), Chief Information Officer (CIO), "Software Development and Open Source Software," January 24, 2022, https://dodcio.defense.gov/portals/0/documents/library/softwaredev-opensource.pdf
[197] Splunk, "Log4Shell – Detecting Log4j 2 RCE Using Splunk," December 9, 2021, https://www.splunk.com/en_us/blog/security/log-jammin-log4j-2-rce.html
[198] SANS Internet Storm Center (ISC) InfoSec Forums, "RCE in log4j, Log4Shell, or how things can get bad quickly," December 10 2021, https://isc.sans.edu/forums/diary/RCE+in+log4j+Log4Shell+or+how+things+can+get+bad+quickly/28120/
[199] CrowdStrike, "Log4j2 Vulnerability 'Log4Shell' (CVE-2021-44228)," December 10, 2021, https://www.crowdstrike.com/blog/log4j2-vulnerability-analysis-and-mitigation-recommendations/
[200] Palo Alto Networks (PAN), "CVE-2021-44228 Impact of Log4j Vulnerability," December 10, 2021, https://security.paloaltonetworks.com/CVE-2021-44228
[201] Microsoft 365 Defender Threat Intelligence Team and Microsoft Threat Intelligence Center (MSTIC), Microsoft Security, "Guidance for preventing, detecting, and hunting for exploitation of the Log4j 2 vulnerability," December 11, 2021, https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/

- December 11, 2021 – Google released guidance on a new preconfigured WAF rule for Google Cloud Armor.[202]
- December 13, 2021 – Google published another advisory with recommendations for investigating and responding to Log4j with Google Cloud.[203]
- December 15, 2021 – Mandiant released a blog post detailing initial Log4j exploitation and mitigation recommendations.[204]
- December 17, 2021 – Google issued another advisory on Log4j and its impact.[205]
- December 17, 2021 – Flashpoint published a report on threat actor exploitation.[206]

Select Media Communications

Mainstream media also reported on the Log4j event, including technical and situational information.

- December 10, 2021 – The Guardian published an article emphasizing the severity of the vulnerability.[207]
- December 12, 2021 – Bloomberg published a report on the impact of exploitation and its severity.[208]
- December 12, 2021 – The Wall Street Journal reported on the vulnerability and global remediation efforts.[209]
- December 13, 2021 – CNN released a report on the severity of the vulnerability and the software's prevalence.[210]
- December 15, 2021 – Fox News published a report focused on the exploitation efforts of China and Iran-based threat actors.[211]
- December 16, 2021 – The Financial Times reported on open source software concerns.[212]

---

[202] Kiner, Emil and Reisfeld, Dave, Google Cloud, "Google Cloud Armor WAF rule to help mitigate Apache Log4j vulnerability," December 11, 2021, https://cloud.google.com/blog/products/identity-security/cloud-armor-waf-rule-to-help-address-apache-log4j-vulnerability
[203] Google Cybersecurity Action Team, Google Cloud, "Google Cloud recommendations for investigating and responding to the Apache 'Log4j 2' vulnerability," December 13, 2021, https://cloud.google.com/blog/products/identity-security/recommendations-for-apache-log4j2-vulnerability
[204] Hultquist, John and Mcwhirt, Matthew, Mandiant, "Log4Shell Initial Exploitation and Mitigation Recommendations," December 15, 2021, https://www.mandiant.com/resources/log4shell-recommendations
[205] Wetter, James and Ringland, Nicky, Google Open Source Insights Team, "Understanding the Impact of Apache Log4j Vulnerability," December 17, 2021, https://security.googleblog.com/2021/12/understanding-impact-of-apache-log4j.html
[206] Flashpoint, "Log4j Chatter: What Threat Actors Are Sharing About the Log4Shell Vulnerability," December 17, 2021, https://www.flashpoint-intel.com/blog/log4j-chatter/
[207] The Guardian, "Recently uncovered software flaw 'most critical vulnerability of the last decade,'" December 10, 2021, https://www.theguardian.com/technology/2021/dec/10/software-flaw-most-critical-vulnerability-log-4-shell
[208] Gillum, Jack, Bloomberg, "Companies Rush to Fix Software Exploit After U.S. Warning," December 12, 2021, https://www.bloomberg.com/news/articles/2021-12-12/companies-rush-to-fix-software-exploit-after-u-s-warning
[209] McMillan, Robert, The Wall Street Journal, "Software Flaw Sparks Global Race to Patch Bug," December 12, 2021, https://www.wsj.com/articles/tech-giants-microsoft-amazon-and-others-warn-of-widespread-software-flaw-11639260827
[210] Lyngaas, Sean, Cable News Network (CNN), "DHS warns of critical flaw in widely used software," December 13, 2021, https://www.cnn.com/2021/12/11/politics/dhs-log4j-software-flaw-warning/index.html
[211] Fox News Channel (FNC), "Chinese and Iranian hackers exploit Log4j computer flaw, affecting hundreds of millions," December 15, 2021, https://www.foxnews.com/tech/chinese-iranian-hackers-exploit-log4j-computer-flaw
[212] Financial Times, "Log4j hack raises serious questions about open source software," December 16, 2021, https://www.ft.com/content/73df7fde-5800-4676-bfb4-9832157758be

APPENDIX E: OBSERVATIONS ON THE OPEN SOURCE SOFTWARE ECOSYSTEM

The Board studied the open source ecosystem's current secure software development practices and learned about efforts to help sustain or improve such practices. This appendix captures additional observations not cited in the main report that warrant acknowledgement.

Open source development is a community-based volunteer effort that places importance on participation from a variety of developers. Accordingly, this model does not always promote security fundamentals.[213] Due to their myriad of backgrounds and skill levels, developers may not be familiar with secure coding principles, particularly if certifications and curricula do not provide this training.[214] Open source developers are often volunteers with full time jobs and contribute to open source projects in their free time, fulfilling tasks based on their interests, skills, and expertise, which may not align with recognized secure coding practices.[215]

To address these gaps, many open source software foundations provide support at the developer-level and encourage a cultural shift that prioritizes security. For example, some organizations maintain programs to reward developers who obtain security-related certifications.[216] Another non-profit organization entrusts safekeepers or evangelists to manage community oversight.[217, 218] ASF uses a process, called the Attic, to alert users when projects are no longer maintained so users are aware that continued use may introduce risk.[219, 220] The Linux Foundation maintains active resources that inform developers of secure software development practices.[221]

Organizations with resource capacity also fund and support open source software foundations. OpenSSF launched the Alpha-Omega project in February 2022 to improve open source software security by helping project maintainers search for and fix undiscovered vulnerabilities in 10,000 commonly deployed projects.[222] Two technology services companies gave a $5 million initial investment to the project[223] and both pledged millions of dollars in open source project funding.[224, 225]

---

[213] Chief Information Security Officer (CISO); Technology services company. Subcommittee Meeting.
[214] Manager; Software Engineering Institute (SEI), Carnegie Mellon University (CMU). Subcommittee Meeting.
[215] Log4j Logging team; Apache Software Foundation (ASF). Subcommittee Meeting.
[216] Chief Information Security Officer (CISO); Technology services company. Subcommittee Meeting.
[217] Senior director; Non-profit organization. Subcommittee Meeting.
[218] Similar to this model, the Atlantic Council's 2021 report on the Solarwinds' Suburst compromise suggests DHS CISA create Open Source Security Teams to adapt the federal cyber risk management system. But there is a lack of quantitative evidence that implementing this position would have a measurable impact on improving vulnerability mitigation, or that it would have created an improved process for discovering and mitigating the Log4j vulnerability. *Source: Herr, Trey et al., Atlantic Council, "Broken trust: Lessons from Sunburst," March 29, 2021, https://www.atlanticcouncil.org/in-depth-research-reports/report/broken-trust-lessons-from-sunburst/#improvedefensibility*
[219] Leadership and Security team; Apache Software Foundation (ASF). Board Meeting.
[220] Apache Software Foundation (ASF), "Moving a PMC to the Attic," https://attic.apache.org/process.html
[221] Linux Foundation (LF), https://training.linuxfoundation.org/blog/
[222] Open Source Security Foundation (OpenSSF), "OpenSSF Announces The Alpha-Omega Project to Improve Software Supply Chain Security for 10,000 OSS Projects," February 1, 2022, https://openssf.org/press-release/2022/02/01/openssf-announces-the-alpha-omega-project-to-improve-software-supply-chain-security-for-10000-oss-projects/
[223] Open Source Security Foundation (OpenSSF), "OpenSSF Announces The Alpha-Omega Project to Improve Software Supply Chain Security for 10,000 OSS Projects," February 1, 2022, https://openssf.org/press-release/2022/02/01/openssf-announces-the-alpha-omega-project-to-improve-software-supply-chain-security-for-10000-oss-projects/
[224] Technology services company. Response to Board request for information.
[225] Technology services company. Response to Board request for information.

APPENDIX F: PRACTICES CONTRIBUTING TO EVENT RESPONSE AND MANAGEMENT

During its review, the CSRB heard insights into the practices organizations leveraged to manage the risks and threats associated with the Log4j event. This section examines characteristics of communication, vulnerability identification, risk mitigation, and threat monitoring that contributed to effective response.

Communication

Private sector vendors, defenders, and U.S. government entities, including CISA, JCDC, NSA, and the FBI,[226] leveraged several techniques to communicate emerging and actionable information surrounding Log4j risks.[227] Responders relied on these collaboration efforts to inform awareness of the severity and potential impact of the Log4j vulnerability and provide identification, detection, mitigation, and protection guidance.[228]

Vendors primarily distributed communications through subscription-based services or publicly downloadable content on their websites, while government agencies deployed information across dedicated websites and indicator platforms. Communication techniques also employed crowdsourcing capabilities by leveraging social media, namely Twitter, to maximize the reach, timeliness, and validation of emerging Log4j-related details.[229, 230]

Vulnerability Identification

To overcome the challenges associated with identifying potentially affected assets, organizations enlisted a variety of automated and manual tools to search for vulnerable components, inform the scope of Log4j within their environment, and assess their level of exposure.[231, 232] Throughout this process, responders leveraged scanning tools, endpoint detection and response (EDR) solutions, vendor-provided and custom-developed scripts, and other security testing tools.

Organizations with penetration testing and threat hunting capabilities deployed additional resources to probe selective parts of the environment manually. This process enabled them to gain supplemental visibility into their attack surface and evaluate their exposure, further enabling them to prioritize risks and develop patch prioritization plans.

Risk and Threat Management

To minimize Log4j vulnerability exposure, risk management teams patched vulnerable components and implemented compensating controls. When patches were not available, organizations operationalized various remediation techniques.[233]

Many organizations leveraged additional defense capabilities by updating WAF configurations, deploying signatures to intrusion detection and prevention systems (IDS/IPS), and updating threat detection rules to expose exploitation attempts. Defenders primarily leveraged security incident event management (SIEM), EDR,[234] and managed detection and response (MDR) capabilities[235] to ingest and process security information, telemetry, logs, IOCs,[236] and threat intelligence.[237] These capabilities provided opportunities for

---

[226] Cybersecurity and Infrastructure Security Agency (CISA), "CISA, FBI, NSA and International Partners Issue Advisory to Mitigate Apache Log4j Vulnerabilities," December 22, 2021, https://www.cisa.gov/news/2021/12/22/cisa-fbi-nsa-and-international-partners-issue-advisory-mitigate-apache-Log4j
[227] Senior executive; Cybersecurity technology services company. Subcommittee Meeting.
[228] Federal Chief Information Security Officer (CISO). Subcommittee Meeting.
[229] Federal Bureau of Investigation (FBI) (@FBI), Twitter, December 22, 2021, https://twitter.com/FBI/status/1473681715730202627
[230] National Security Agency (NSA) Cybersecurity (@NSACyber), Twitter, December 22, 2021, https://twitter.com/NSACyber/status/1473680239087824901
[231] Chief Information Security Officer (CISO); Critical infrastructure sector company. Subcommittee Meeting.
[232] Federal Chief Information Security Officer (CISO). Response to Board request for information.
[233] Federal Chief Information Security Officer (CISO). Response to Board request for information.
[234] Cybersecurity technology services company. Response to Board request for information.
[235] Federal Chief Information Security Officer (CISO). Response to Board request for information.
[236] Cybersecurity technology services company. Response to Board request for information.
[237] Senior executive; Cybersecurity technology services company. Subcommittee Meeting.

incident response and vulnerability intelligence teams to share information, and enabled response teams to visualize and neutralize threats.[238]

[238] Senior analyst; Cybersecurity technology services company. Subcommittee Meeting.

APPENDIX G: CYBER SAFETY REVIEW BOARD MEMBERS

The following members participated in this inaugural review of the Cyber Safety Review Board.

Robert Silvers, Under Secretary for Policy, Department of Homeland Security (Chair)

Heather Adkins, Senior Director, Security Engineering, Google (Deputy Chair)

Dmitri Alperovitch, Co-Founder and Chairman, Silverado Policy Accelerator and Co-Founder and former Chief Technology Officer (CTO) of CrowdStrike, Inc.

John Carlin, Principal Associate Deputy Attorney General, Department of Justice

Chris DeRusha, Federal Chief Information Security Officer, Office of Management and Budget

Chris Inglis, National Cyber Director, Office of the National Cyber Director

Rob Joyce, Director of Cybersecurity, National Security Agency

Katie Moussouris, Founder and CEO, Luta Security

David Mussington, Executive Assistant Director for Infrastructure Security, Cybersecurity and Infrastructure Security Agency

Chris Novak, Co-Founder and Managing Director, Verizon Threat Research Advisory Center

Tony Sager, Senior Vice President and Chief Evangelist, Center for Internet Security

John Sherman, Chief Information Officer, Department of Defense

Bryan Vorndran, Assistant Director, Cyber Division, Federal Bureau of Investigation

Kemba Walden, Assistant General Counsel, Digital Crimes Unit, Microsoft[239]

Wendi Whitmore, Senior Vice President, Unit 42, Palo Alto Networks

[239] Member's affiliation changed to the Office of the National Cyber Director on June 6, 2022.

APPENDIX H: ACRONYMS

AAU	Association of American Universities
AAUP	American Association of University Professors
ABET	Accreditation Board for Engineering and Technology
ACE	American Council on Education
APLU	Association of Public Land Grant Universities
APT	Advanced Persistent Threat
ASF	Apache Software Foundation
BOD	Binding Operational Directive
BSI	Federal Office for Information Security of Germany
CCE	Common Configuration Enumeration
CERT	Community Emergency Response Team
CERT/CC	Community Emergency Response Team - Coordination Center
CERT-EU	Computer Emergency Response Team - EU
CI/CD	Continuous Integration/Continuous Delivery
CIO	Chief Information Officer
CIPAC	Critical Infrastructure Partnership Advisory Council
CIRCIA	Cyber Incident Reporting for Critical Infrastructure Act of 2022
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CMDB	Configuration Management Database
CPE	Common Platform Enumeration
CSAB	Computer Sciences Accreditation Board
C-SCRIP	Communication Supply Chain Risk Information Partnership
CSIRT	Computer Security Incident Response Teams
CSRB; the Board	Cyber Safety Review Board
CSRS	Cyber Safety Reporting System
CTO	Chief Technology Officer
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
DoD	Department of Defense
DoS	Denial-of-Service
E.U.	European Union

ED	Emergency Directive
EDR	Endpoint Detection and Response
ENISA	European Union Agency for Cybersecurity
EO	Executive Order
E.U.	European Union
FAR Council	Federal Acquisition Regulatory Council
FBI	Federal Bureau of Investigation
FIRST	Forum of Incident Response and Security Teams
FTC	Federal Trade Commission
GAO	U.S. Government Accountability Office
GovCERT	Government Computer Emergency Response Team
HLC	Higher Learning Commission
ICS	Industrial Control Systems
IDE	Integrated Development Environment
IDS	Intrusion Detection System
INCD	Israel National Cyber Directorate
IOC	Indicator of Compromise
IoT	Internet-of-Things
IPS	Intrusion Prevention System
ISAC	Information Sharing and Analysis Centers
ISAO	Information Sharing and Analysis Organizations
ISC	Internet Storm Center
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
JCDC	Joint Cyber Defense Collaborative
JNDI	Java Naming and Directory Interface™
KEV	Known Exploited Vulnerability
LDAP	Lightweight Directory Access Protocol
MDR	Managed Detection and Response
MIIT	Ministry of Industry and Information Technology
MPS	Ministry of Public Security
MTTR	Mean Time to Repair
NASA	National Aeronautics and Space Administration
NCAE-C	National Centers of Academic Excellence in Cybersecurity
NCCIC	National Cybersecurity and Communications Integration Center

NCSC-UK	National Cyber Security Centre of the U.K.
NCSC-NL	National Cyber Security Centre of the Netherlands
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSF	National Science Foundation
NVD	National Vulnerability Database
OISF	Open Information Security Foundation
OMB	Office of Management and Budget
ONCD	Office of the National Cyber Director
OpenSSF	Open Source Security Foundation
OWASP	Open Web Application Security Program
PRC	People's Republic of China
PSIRTs	Product Security Incident Response Teams
SANS	SANS Institute
SBOM	Software Bill of Material
SIEM	Security Incident Event Management
SSRACE	Software Security Risk Assessment Center of Excellence
TTPs	Tactics, Techniques, and Procedures
U.K.	United Kingdom
VINCE	Vulnerability Information and Coordination Environment
WAF	Web Application Firewall