Testimony of Brad Arkin, Senior Vice President, Chief Security and Trust Officer, Cisco Systems
Before Senate Homeland Security and Governmental Affairs Committee
Responding to and Learning from the Log4Shell Vulnerability
Tuesday, February 8, 2022, 10 AM Eastern
Senate Dirksen Office Building, SD-342

Introduction

Chairman Peters, Ranking Member Portman, and Members of this Committee, thank you for the invitation to speak with you today and for your leadership on the important issues we are discussing—including our collective response to and learnings from the Log4j vulnerability.

My name is Brad Arkin, and I am the Chief Security and Trust Officer for Cisco Systems. I am responsible for the security of our company as well as our products and services. Today, I am going to discuss our experience with the Log4j vulnerability, how Cisco responded to help protect our enterprise and our customers, how the U.S. federal government can play an important role in supporting cybersecurity efforts across industry, and important lessons we have learned. Together, we need to further improve: 1) baselines for software security, including open source software; 2) speed and efficiency at finding and fixing problems when they arise; and 3) resilience against attacks, particularly in the window between identification of a vulnerability and application of a fix or mitigation.

Cisco: A Worldwide Leader in Security for Software, Cloud, Networking, and Applications

While Cisco built its reputation as a networking hardware company, we are now one of the largest software companies in the world, with $15 billion in software revenue in 2021.[1] Our portfolio is

[1] https://www.cisco.com/c/dam/en_us/about/annual-report/cisco-annual-report-2021.pdf

one of the broadest in the technology industry and includes software, Software-as-a-Service (SaaS), hardware, silicon, and services. Software is central to Cisco's business and can be found in our supply chain, cloud products, cloud-enabled hardware, traditional networking hardware, and enterprise IT environments.

Cisco is an important technology partner to the U.S. government, as part of the Defense Industrial Base (DIB), and a central technology provider to critical infrastructure companies, including financial services, healthcare, energy, manufacturing, and businesses of all sizes. Cisco is a global company with nearly 80,000 full-time employees located worldwide. We own and operate a large, complex IT environment to run our business and support our customers. Protecting our company, our customers, and their data from cyber-attacks is critical to our business.

Discovery, Response, and Remediation of the Log4j Vulnerability

On December 9, 2021, a critical vulnerability was revealed in the Log4j library used in almost every java application written and used on the Internet. The Log4J library is commonly used in the development of software when logging is needed on a variety of systems. This library intentionally includes the ability for a programmer to remotely fetch executable code from a remote server and execute it. The vulnerability discovered allowed remote attackers to force a vulnerable system to use this functionality without the knowledge or permission of its owner and, thereby, download and run malicious code. Additional vulnerabilities related to Log4j were discovered in subsequent weeks.

This created an industry-wide problem, as organizations around the world needed to figure out how they were using Log4j, the potential exposure that needed to be addressed, and how they could best manage the associated risks. For Cisco, the scope and diversity of our technology business made our Log4j response complex, requiring us to identify the presence of the vulnerability as well as apply necessary fixes, using risk assessments to drive prioritization of this work.

In 2014, our industry faced a similarly widespread zero-day vulnerability called “Heartbleed.” At that time, it took Cisco 50 days to identify the full list of software that required updates to remediate the vulnerability and several additional weeks to apply the necessary software patches. With our Log4j response, Cisco was able to respond significantly faster and was able to identify the use of the Log4j library within its products and services and provide software patches for affected products within 10 days. This significant improvement in response time was helped by lessons learned in the past, Cisco’s on-going security efforts, and the collaborative efforts facilitated by partnerships, including the Joint Cyber Defense Collaborative (“JCDC”).

By focusing on historical lessons learned, building better and more secure software, and having data about which specific applications and software we use, we were able to move quicker, eliminate risk faster, and have the agility needed to manage our own security and resilience. For Cisco, the key differentiator was our improved visibility into the software applications and third-party products that we use as a company. Additionally, we now use tooling to allow us to see the software maintenance status of the applications we use, identifying whether a particular piece of software is the latest version. We strongly recommend the use of tools and technology that allow companies and government agencies to have this kind of visibility into the applications they employ and their maintenance status. Those tools and technologies must then also be anchored by mature incident management processes and capabilities.

Many important investments for Cisco—such as our internal source code scanning capabilities, our Zero trust network architecture, and our ability to isolate within our networks—helped drive efficacy during this event. We will continue to review this event and integrate what we learn into future investments to bolster future remediation efforts.

Government Support During the Log4j Vulnerability

Throughout the incident, we actively exchanged cyber threat intelligence with both our industry peers and government including through the JCDC stood up by Department of Homeland Cybersecurity and Infrastructure Agency ("CISA") Director Jen Easterly this past year. The JCDC is intended to satisfy a requirement from Congress that CISA facilitate joint cyber planning and coordination with the private sector. The shared learnings from these engagements provided us insight into the evolving nature of the threats and helped guide our risk decisions internally. Cisco updated public-facing materials on a regular basis to keep our customers aware of the potential impact of the vulnerability on Cisco products and services and to give them specific mitigation information. These experiences demonstrate that private sector risk prioritization efforts greatly benefit from the government sharing readily actionable cyber threat information at the lowest possible classification, which then enables their rapid, timely, and widespread dissemination.

Tight integration within our security function and threat intelligence from Cisco Talos helped us to effectively prioritize remediation efforts. At Cisco, we are fortunate to have a world-class threat intelligence function like Cisco Talos and the resources to create a robust response to Log4j. But even smaller companies without our sophisticated threat intelligence capabilities can benefit from CISA's public awareness campaigns. Their ability to access information from CISA will prove vital as they struggle to understand the risks they face, whether and how active exploits are occurring, and where to focus their remediation resources.

In my view, CISA correctly identified an important approach when it issued Binding Operational Directive 22-01 last year, which requires agencies to expedite patching of known vulnerabilities that are being actively exploited. Earlier this year, CISA then began publishing a catalog of these known exploited vulnerabilities with a specific timeline for their expected remediation. Active and ongoing patching is an important way to mitigate cyber risks and prevent the exploitation of vulnerabilities. This is consistent with the conclusions of Cisco’s own research.[2] Organizations must prioritize risk differently than they have in the past.

Software Security and the Use of Open Source Software

All software has the potential to contain vulnerabilities, and we need to build and maintain software and systems to be resilient in the face of these vulnerabilities. Efforts to improve software quality and reduce the frequency and impact of security vulnerabilities are important, but there will always be security bugs in software developed by humans. Tools, like software bills of materials (“SBOMs”), have the potential to help coordinate efforts across the entire ecosystem to make it easier to achieve good outcomes despite the inevitable presence of these vulnerabilities. For that reason, we applaud the steps laid out in Executive Order 14028 and the work NIST is doing in areas like the development of the Secure Software Development Framework.

[2] A report containing Cisco Kenna’s research on this issue may be found here: https://www.kennasecurity.com/resources/prioritization-to-prediction-report-volume-eight/

It is my opinion that open source software did not fail, as some have suggested, and it would be misguided to suggest that the Log4j vulnerability is evidence of a unique flaw or increased risk with open source software. The truth is that all software contains vulnerabilities due to inherent flaws of human judgment in designing, integrating, and writing software. Cisco has a well-developed Product Security Incident Response Team ("PSIRT") process to help manage that risk, apply necessary patches, and help our customers perform the necessary remediation once we learn of their existence. Cisco's Talos Threat Intelligence team also provides vital information about vectors of attack and indications of actual exploitation and compromise "in the wild."[3]

Cisco is a significant user of and an active contributor to open source security projects. These are important efforts necessary to maintain the integrity of code blocks shared across foundational elements of IT infrastructure. However, I believe that focusing narrowly on the risks posed by open source software may distract us from other significant areas where we can address security risks inherent in all software.

Indeed, we strive to ensure that all the software we use and provide our customers only gets better and is increasingly secure. This is done through the extensive use of a Secure Development Lifecycle ("SDL"), which documents mandatory policies and practices to reduce risks throughout the anticipated span of use for a product or service. Cisco's SDL is informed by our decades of experience and learnings in software development. Ensuring that the environment in which the software is written, compiled, and deployed is highly secure is also an essential practice. It helps us to ensure that software from different components follow rigorous processes that include

[3] https://blog.talosintelligence.com/2021/12/apache-log4j-rce-vulnerability.html

hardening, vulnerability management, logging and monitoring, segmentation, and access controls.

Equally important are ways that we mitigate the risks of vulnerable software by building our IT systems and our infrastructure to limit the “blast radius” of any potential vulnerability. Highly secure architectures are critical to creating the necessary separation inside of systems to limit the impact of exploitable vulnerabilities and enable rapid recovery and resiliency. Proper segmentation, for example, makes it difficult for an attacker to move laterally through the network, even if they can gain initial access by exploiting a vulnerability. Implementing a zero-trust environment further protects critical data and systems from intrusion and exploitation by ensuring that every attempt to connect to the network and access important data and systems is examined. We leverage intelligent, automated protective measures that ensure only trusted devices are being used and that their users have the requisite permission needed to access the specific data, apps, or workloads requested.[4]

We stand a much better chance of managing future discovered vulnerabilities if we acknowledge today the risks inherent in software and focus our energy on using highly secure software build environments, highly secure architectures, and zero-trust strategies.

What Government Can Do to Help

The U.S. government can play an important role in addressing the risks that vulnerabilities pose by creating incentives for companies to have a highly secure and effective way to design and build software, create a highly secure software supply chain, and deliver highly secure code to their

[4] https://www.cisco.com/c/en/us/products/security/zero-trust.html

customers. The government can ensure that critical infrastructure providers—nearly all of whom are important Cisco customers—are securing their critical systems as required.[5]

Executive Order ("EO") 14028 represents an important step that Cisco supports.[6] The emphasis on software security and software transparency (knowing what software ingredients are in the technology we use) are critical points of focus in the EO. We want to compliment the work NIST is doing in this area and point the Committee to the NIST Secure Software Development Framework, which presents a comprehensive approach to software security. While this hearing is focused on Log4j and the use of open source software, any successful approach will address the security of all critical software in a holistic way. We must avoid the temptation to concentrate on tactical issues that any close examination of the most recent security event may yield.

Measures like using secure trusted code (to include open source software) as a starting point for code development projects, securing the build environment, providing transparency about software components used through a software bill of materials (SBOM), ensuring a robust process to identify and remediate known vulnerabilities, implementing a process to discover and disclose vulnerabilities to vendors, and quickly disseminating patches to impacted customers once created. Together, these steps will result in a layered approach to software security that will make us more resilient and resistant to the risk of vulnerabilities. Used correctly, SBOMs can help organizations become more agile. They can highlight the need to use current versions of code and allow us to see the risks we may be carrying with greater clarity. This transparency can

[5] See, NERC SIP-13 as an example, at, https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-013-1.pdf

[6] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

facilitate more coordinated ways to collect data and manage vulnerability risks in both proprietary and open source software.

Requiring vendors to publish information about what elements of code are leveraged in a product or service creates a new level of transparency that can allow closer examination of vulnerabilities in software. Understanding risk requires understanding exposure of the necessary facts. SBOMs may help provide an additional important source of data to inform effective, risk-based prioritization of limited resources. The federal government, via the Department of Commerce's National Telecommunications and Infrastructure Administration (NTIA), led efforts to foster private sector development of this concept. It is now being furthered by CISA as a result of the Executive Order. We expect that the federal government will soon begin asking vendors of critical software to supply SBOMs along with other minimum requirements set forth in the Executive Order.

While SBOMs are increasingly part of the assessment and risk management conversation for highly secure software development, I want to caution that they are not the only solution. Furthermore, the processes necessary to produce, publish, and maintain accurate SBOMs are not cost-free. More work needs to be done to ensure the amount of benefit yielded from customer access to SBOMs, and the level of detail they are expected to yield, is worth the amount of time and effort necessary for developers and vendors to produce and maintain them accurately at required levels of specificity and precision.

A Note of Optimism

We typically speak about cybersecurity threats and responses in terms of challenges that remain to be addressed—and without a doubt they are significant. The threat environment is dynamic and constantly evolving. Sophisticated threat actors are highly organized, well-resourced, and closely coordinated. But we are learning, evolving, and coordinating too, and as a result, our ability to manage the risks posed by vulnerabilities is improving in tangible ways. The risks posed by Log4j and subsequent exploits will remain with all of us for quite some time. But the ability of Cisco and others to respond quickly and work together as peer companies and with the government—as well as our collective ability to learn, adapt, and evolve—will allow us to keep raising barriers to the exploitation of vulnerabilities and to malicious cyber activity. For Cisco, our greater speed in responding to Log4j validated years of focus and investment after events like the Heartbleed/OpenSSL vulnerability. The measures discussed today, combined with the benefits we expect from EO 14028, to include SBOMs, will only enhance our ability to respond faster. The industry and the government together must continue to build our collective agility by focusing on the best practices that will enable us to respond to the next important vulnerability event, which will surely come.

Conclusion

In closing, I want to reiterate how much I appreciate the opportunity to testify today and provide Cisco's views on these important topics. Learning lessons from these situations and using events like the Log4j vulnerability response drives improvements. These joint efforts across industry and government help identify new opportunities for continued partnership. Doing so helps raise awareness and capabilities for all organizations, regardless of their size and resources. The Log4j vulnerability demonstrated, yet again, that we are reliant on one another and must continue to work together to manage this ever-present risk. The threat of cyber-attacks and malicious cyber activity, especially by exploiting vulnerabilities, will continue. Transparency, trust, and accountability to one another for protecting and safeguarding critical systems and data must be at the center of our collective cyber response. The U.S. government is uniquely positioned to convene relevant actors together to address this challenge and use its influence to create effective standards and incentives for better software security.