FRANK PALLONE, JR., NEW JERSEY
CHAIRMAN

CATHY McMORRIS RODGERS, WASHINGTON
RANKING MEMBER

ONE HUNDRED SEVENTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927
Minority (202) 225-3641

August 10, 2022

The Honorable Xavier Becerra
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue SW
Washington, DC 20201

Dear Secretary Becerra:

We write to request a briefing from your department related to the open-source software vulnerability—Apache Log4j. The ubiquitous nature of this vulnerability and the hundreds of thousands of known exploits since its disclosure raise concerns about how the United States government is identifying and mitigating potential compromises to its network security.

In late November 2021, a member of the Alibaba Cloud Security Team discovered the Log4j vulnerability and reported the vulnerability to the Apache Software Foundation (ASF).[1] Shortly thereafter, the Cybersecurity and Infrastructure Security Agency (CISA) warned federal agencies that their systems and systems they interface with may be exposed to this vulnerability.[2] After the initial public disclosure, security researchers noticed nation-state threat actors, including China, Russia, Iran, North Korea, and Turkey, attempting to exploit the vulnerability.[3] The Apache Software Foundation released a full solution to the Log4j vulnerability approximately two weeks after the disclosure.[4]

On December 11, 2021, CISA Director Jen Easterly stated that "this vulnerability, which is being widely exploited by a growing set of threat actors, presents an urgent challenge to

---

[1] *Inside the Race to Fix A Potentially Disastrous Flaw*, Bloomberg (Dec. 13, 2021).

[2] Cybersecurity and Infrastructure Security Agency, *Emergency Directive 22-02 Mitigate Apache Log4j Vulnerability* (Dec. 17, 2021) (ED 22-02).

[3] Microsoft, *Guidance for Preventing, Detecting, And Hunting for Exploitation of the Log4j 2 Vulnerability* (Jan. 10, 2022) (www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/); *The Log4j Vulnerability: Millions of Attempts Made Per Hour to Exploit Software Flaw*, Wall Street Journal (Dec. 21, 2021).

[4] Cybersecurity and Infrastructure Security Agency, *Apache Log4J Vulnerability Guidance* (April 8, 2022) (www.cisa.gov/uscert/apache-log4j-vulnerability-guidance).

network defenders given its broad use."[5] She later added, "[t]o be clear, this vulnerability poses a severe risk. We will only minimize potential impacts through collaborative efforts between government and the private sector."[6]

On December 17, 2021, CISA issued Emergency Directive (ED) 22-02 requiring federal civilian departments and agencies to assess their internet-facing network assets for the Apache Log4j vulnerabilities and immediately patch these systems or implement other appropriate mitigation measures.[7] On April 8, 2022, CISA closed ED 22-02 and transitioned the required actions to Binding Operational Directive (BOD 22-01), which means these actions are now mandatory for all federal departments and agencies.[8] Additionally, the Federal Bureau of Investigation asked organizations and agencies to report any compromises that result from the Log4j vulnerability.[9]

Over the past several years, the Committee has done extensive work on cyber threats, including hearings and investigations examining the information-security programs and controls over key computer systems and networks at multiple agencies under the Committee's jurisdiction. Because the Log4j vulnerability is widespread and can affect enterprise applications, embedded systems, and their sub-components, the Committee is seeking to gain a comprehensive understanding of the scope of the vulnerability and actions being taken to mitigate its effects. The risk to federal network security is especially concerning because nation-state threat actors have attempted to exploit this Log4j vulnerability.

Accordingly, we request a staff briefing to discuss your department's response to the Log4j vulnerability by August 24, 2022, including the following questions:

1. When did your department first learn of the Log4j vulnerability?

2. What specific actions has your department taken in response to CISA's guidance in December 2021 and subsequent directive on April 8, 2022, regarding the Log4j vulnerability?

3. What tools does your department employ to detect all instances of the Log4j vulnerability on your networks? What is your department's schedule for identifying the Log4j vulnerability?

---

[5] Cybersecurity and Infrastructure Security Agency*, Statement From CISA Director Easterly on "Log4j" Vulnerability* (Dec 11, 2021).

[6] *Id.*

[7] Cybersecurity and Infrastructure Security Agency, *CISA Issues Emergency Directive Requiring Federal Agencies To Mitigate Apace Log4j Vulnerabilities* (Dec. 17, 2021) (press release).

[8] Cybersecurity and Infrastructure Security Agency *Emergency Directive 22-02 Mitigate Apache Log4J Vulnerability* (April 8, 2022) (ED 22-02).

[9] Federal Bureau of Investigations, *FBI Statement on Log4j Vulnerability* (Dec. 15, 2021) (press release).

a. Does your department track instances of new download of Apache Log4j through the department's network? If so, what steps does the department take to ensure that only patched versions of Log4j are downloaded and utilized?

b. Does your department have a software bill of materials (S-BOM) that identifies all of its assets? If so, how often is it updated?

4. Does your department employ software that utilizes Apache Log4j? If so, how many software products employed by the department include the Log4j vulnerability?

   a. How many of those software products have adopted the patch for the Log4j vulnerability?

   b. What actions is your department taking to engage with private sector partners to provide recommended practices for patch management of the Log4j vulnerability?

5. Has your department been impacted by a compromise or exploitation of the Log4j vulnerability? If so, when was your department first compromised, when did you detect the compromise, what was the extent of the compromise, and how did the department address the compromise?

6. What incident alert thresholds does your department have for potential compromises generally, and what are your requirements for escalating and reporting anomalies?

7. Does your department have a specific plan to identify and remediate, on an ongoing basis, software that it uses to ensure the department is not currently using software vulnerable to a cyber threat?

Your assistance in this urgent matter is appreciated. If you have any questions, please contact Alan Slobodin of the Minority Committee staff and Will McAuliffe of the Majority Committee staff.

Sincerely,

Frank Pallone, Jr.
Chairman

Cathy McMorris Rodgers
Ranking Member

Diana DeGette
Chair
Subcommittee on Oversight
and Investigations

H. Morgan Griffith
Ranking Member
Subcommittee on Oversight
and Investigations

Anna G. Eshoo
Chairwoman
Subcommittee on Health

Brett Guthrie
Ranking Member
Subcommittee on Health