

FRANK PALLONE, JR., NEW JERSEY
CHAIRMAN

CATHY McMORRIS RODGERS, WASHINGTON
RANKING MEMBER

ONE HUNDRED SIXTEENTH 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

February 28, 2022

The Honorable Lina Khan
Chairwoman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Chairwoman Khan:

We are closely following the news of the discovery of vulnerability in the open-source software known as Apache Log4j. We are also aware that on January 4, 2022, the Federal Trade Commission (FTC) warned in a blog post that it “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 the Log4j vulnerability, or similar known vulnerabilities in the future”¹.

We appreciate that you share our commitment to data security and hope this is a sign that your agency, the Biden Administration, and Congressional Democrats finally will support a bipartisan privacy and data security solution, much like Republican members of the Energy and Commerce Committee outlined in the “Control Our Data Act” last November. The “go-it-alone” approach that Democrats have followed since President Biden’s inauguration has either failed or contributed to severe, negative consequences. Despite the temptation, we encourage you to work with us instead of trying to contort existing FTC authorities to achieve your policy goals.

We also note that the Cybersecurity and Infrastructure Security Agency (CISA) recently warned federal agencies that their systems and systems they interface with may be exposed to

¹ Federal Trade Commission, *FTC warns companies to remediate Log4j security vulnerability* (Jan 4, 2022) available at: <https://www.ftc.gov/news-events/blogs/techftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability>

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. The Apache Software Foundation released a full solution to the Log4j vulnerability approximately two weeks after the disclosure.

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 network defenders given its broad use.”³ 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.”⁴

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.⁵ Additionally, the Federal Bureau of Investigation (FBI) asked organizations and agencies to report any compromises as the result of the Log4j vulnerability.⁶

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 fuller 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, please provide written answers and any necessary documentation to the following questions by March 7, 2022:

1. Does your agency employ Apache Log4j? If so, how many software products employed by the agency include the Log4j vulnerability?
2. How many of those software products have adopted the patch for the Log4j vulnerability?

² Cybersecurity and Infrastructure Security Agency, *Emergency Directive 22-02 Mitigate Apache Log4j Vulnerability* (Dec 17, 2021) available at: <https://www.cisa.gov/emergency-directive-22-02>

³ Cybersecurity and Infrastructure Security Agency, *Statement From CISA Director Easterly on “Log4j” Vulnerability*, (Dec 11, 2021) available at: <https://www.cisa.gov/news/2021/12/11/statement-cisa-director-easterly-log4j-vulnerability>

⁴ *Id.*

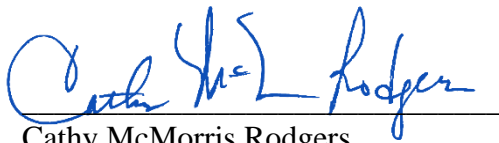
⁵ Cybersecurity and Infrastructure Security Agency, *CISA Issues Emergency Directive Requiring Federal Agencies To Mitigate Apache Log4j Vulnerabilities*, (Dec 17, 2021) available at: <https://www.cisa.gov/news/2021/12/17/cisa-issues-emergency-directive-requiring-federal-agencies-mitigate-apache-log4j>

⁶ Federal Bureau of Investigations, *FBI Statement on Log4j Vulnerability*, (Dec 15, 2021) available at: <https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-log4j-vulnerability>

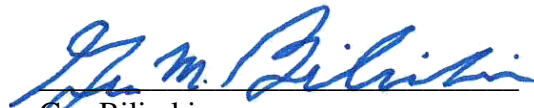
3. Do you know the number of recent downloads of Apache Log4j within your agency? Do these recent downloads of Apache Log4j contain the Log4j vulnerability?
4. What is your agency's schedule for identifying and mitigating any Log4j vulnerabilities?
5. Does your agency have a software bill of materials (S-BOM) that identifies all of its assets? If so, how often is it updated and does it contain Apache Log4j?
6. When did your agency first learn of the Log4j vulnerability? What incident alert thresholds does your agency have, and what are your requirements for escalating and reporting anomalies?
7. Does your agency have a specific plan to identify and remediate, on an ongoing basis, software that it uses to ensure the agency 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 Brannon Rains and Marissa Gervasi on the committee staff.

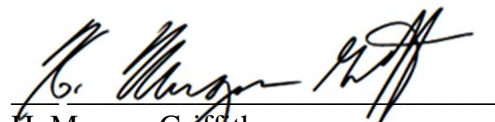
Sincerely,



Cathy McMorris Rodgers
Republican Leader



Gus Bilirakis
Republican Leader
Subcommittee on Consumer Protection
and Commerce



H. Morgan Griffith
Republican Leader
Subcommittee on Oversight
and Investigations