Regulatory Risks of the Log4j Vulnerability: FTC Warns Companies to Take Reasonable Steps to Protect Consumer Data

January 10, 2022

Be prepared for increasing scrutiny from the Federal Trade Commission ("FTC") and other regulators regarding the Log4j vulnerability. The attention of the cybersecurity community has been captured by the recently disclosed critical vulnerability in the widely used, open-source Java logging package, Log4j (CVE-2021-44228), and other subsequently announced related vulnerabilities, which is reportedly being "widely exploited" by attackers and "poses a severe risk," according to the Cybersecurity & Infrastructure Security Agency ("CISA") and other technical experts. CISA issued Emergency Directive 22-02 on December 17, 2021, which directs federal civilian executive branch agencies to address Log4j vulnerabilities immediately through patching or other mitigation measures. And now regulators, most notably the FTC, have begun to issue positions on the need for companies and their vendors to remediate the Log4j vulnerability and the enforcement risks that could be presented if a company or its vendors fail to do so.

On January 4, 2022, the FTC's Chief Technology Officer ("CTO") and Division of Privacy and Identity Protection ("DPIP") staff as well as the Artificial Intelligence ("AI") Strategy team, published a blog post titled, *FTC warns companies to remediate Log4j security vulnerability*. In the blog post, the FTC reiterates the risks of loss or breach of personal information, financial loss and other irreversible harms presented by vulnerabilities that are discovered and exploited. The FTC also underscores that companies have a duty to take reasonable steps to mitigate known software vulnerabilities based on potentially applicable laws, such as the Federal Trade Commission Act and the Gramm Leach Bliley Act. The FTC therefore urges companies and their vendors using Log4j to act now "in order to reduce the likelihood of harm to consumers, and to avoid FTC legal action," and further explains 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."

The FTC's January 4 blog post provides steps that companies and their vendors should take to address the vulnerability. As an initial step, a company and its vendors should check to see if they use the Log4j software library by consulting the CISA guidance page.

In addition, CISA is regularly updating a GitHub repository with a list of affected vendors and products. CISA also has information on cyber resources, including scanning software, and provides a cyber hygiene program. If a company or its vendors do use the Log4j software library, according to the FTC, they should:

- Update the Log4j software package to the most current version on Apache's page;
- Consult CISA guidance to mitigate this vulnerability;
- Ensure remedial steps are taken to ensure that companies and their vendors' practices do not violate the law. Failure to identify and patch instances of this software may violate the FTC Act; and
- Distribute this information to any relevant third-party subsidiaries that sell products or services to consumers who may be vulnerable. The FTC has demonstrated that it is serious about data security issues and holding companies accountable for protecting consumer data, especially issues presented by known security vulnerabilities and companies' failures to implement reasonable patch and vulnerability management programs and safeguards. Since 2002, as the Commission noted in its 2020 *Report on Resources Used and Needed for Protecting Consumer Privacy and Security*, the FTC has brought more than 70 cases against companies that have engaged in unfair or deceptive practices that included inadequate protection of consumers' personal data.

In 2019, the FTC strengthened its standard orders in data security cases by (1) making them more specific with respect to the security safeguards that must be implemented to address the complaint's allegations; (2) increasing third-party assessor accountability; and (3) elevating data security considerations to the executive and board levels. These data security order enhancements were reflected in seven orders announced in 2019 and notably included the global settlement with Equifax. The 2019 FTC data security orders focused on a broad range of companies: a pay-to-click survey company; operators of an online rewards website and a dress-up games website; a car dealer software provider; a computer networking equipment manufacturer regarding its wireless routers and Internet cameras; and a service provider providing back-end operation services to multi-level marketers.

Companies and their vendors should take notice of the FTC's January 4 warning regarding Log4j and ensure that they are actively taking steps to remediate the Log4j vulnerability as well as to enhance their data security programs in response to the associated evolving threat landscape.

The authors would like to thank Debevoise & Plimpton law clerk Kathryn Mueller for her contribution to this article.

* * *

To subscribe to our Data Blog, please click here.

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com

NEW YORK

Avi Gesser
agesser@debevoise.com

Michael R. Roberts
mrroberts@debevoise.com