BRACEWELL

INSIGHTS

FTC Warns Use of "Full Legal Authority" on Companies That Ignore Log4j Risk

January 10, 2022

The Federal Trade Commission (FTC) sent a strong message to organizations in the wake of the ***Log4j security vulnerability***: patch now or face regulatory scrutiny and potential legal action.

In the ***notice issued last week***, the FTC acknowledged and emphasized that the Log4j vulnerability is being exploited by a growing set of attackers, which "risks a loss or breach of personal information, financial loss, and other irreversible harms." The FTC made clear that, pursuant to federal laws such as the Federal Trade Commission Act and the Gramm-Leach-Bliley Act, organizations have "a duty to take reasonable steps to mitigate known software vulnerabilities." Finally, the FTC cited to prior enforcement actions and stated that the agency will not hesitate 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 isn't the only regulator with Log4j on its radar: the Securities and Exchange Commission (SEC) issued a "***spotlight***" on the vulnerability stating that "CISA and its partners are responding to active, widespread exploitation of a critical remote code execution vulnerability in Apache's Log4j software library." The SEC has a demonstrated track record of bringing ***enforcement actions*** against public companies for deficient disclosure and controls related to cybersecurity risks and incidents, including instances where ***companies failed to remediate known vulnerabilities***.

As Log4j continues to grow in use and impact, organizations that believe they or their vendors might utilize the Log4j software should immediately review the ***Log4j Vulnerability Guidance*** issued by CISA and determine whether any remediation is necessary. And, for those organizations that have already taken remedial measures, or are in the process of doing so, they should ensure that all remedial steps have been adequately documented in anticipation of questions from regulators or other stakeholders. In order to avoid regulatory scrutiny, organizations should also ensure they maintain information security policies and procedures in line with their legal obligations and that reflect the evolving threat landscape.

Companies with additional questions about the Log4j vulnerability and its potential impact on technical threats and potential regulatory scrutiny or commercial liability are encouraged to contact outside cybersecurity counsel.