Freeborn

New Cyber-Attack Vector, Log4Shell: One of the Most Concerning Exploits Needs to Be On Your Radar

by Joel B. Bruckman

A FREEBORN & PETERS LLP CLIENT ALERT

Last week, a new exploit affecting the very commonly used Apache logging framework, "Log4j 2" (a Java based logging utility), came to light. This attack vector is being referred to as Log4Shell. Some of the most commonly used software programs including those offered by Amazon, IBM, Microsoft, Cisco, and VMWare are affected by this newly discovered vulnerability. Initial reports suggest that hackers have been exploiting this vulnerability since the beginning of the month, according to Cisco. To be clear, this code is used in software of all sorts. This past Friday, Jen Easterly, Director of the US Cybersecurity and Infrastructure Security Agency, warned that "this vulnerability poses a severe risk… [to] the wide array of products using this software."

What is most concerning about this new threat beyond the extent to which the vulnerable code is used in a variety of enterprise software, is the vast capability of those who use the exploit as a catalyst for cyber-attacks. At bottom, this vulnerability allows hackers to take over computers and use those compromised systems as they choose. Hackers are able to do this by creating and implementing their own code into the Apache framework. That code may allow the hackers to use the hi-jacked computer to conduct crypto-mining campaigns, harvest user ,credentials, and exfiltrate data, according to a report published by Microsoft. Such unauthorized access or exfiltration to data may trigger legal obligations. Whether those obligations are statutory, regulatory or contractual they likely require swift action in response to the discovery of a data-security incident, including triage investigation, risk-analysis, and in certain cases notification to those whose information may be at risk.

Jen Easterly, Director of the US Cybersecurity and Infrastructure Security Agency warned that "this vulnerability poses a severe risk… [to] the wide array of products using this software."

As of yesterday, Microsoft has updated its initial report to reflect that it has identified and is actively monitoring several threat actors conducting mass scans for the Log4j vulnerability to levy a Log4Shell cyber-attack. Those efforts have identified several nation-state actors including China, Iran, North Korea and Turkey. Microsoft continues to roll out tools through its Microsoft 365 Defender application to try to identify software on systems which contain the Log4j vulnerability.

All businesses must be aware and vigilant in defending against this new significant threat in order to prevent data security incidents. CISOs, Directors of IT and CTOs must take proactive measures to ensure that they are mitigating the risk of unauthorized access to their company's systems and data.

If you do not have an Incident Response Plan in place, or have questions regarding this new attack vector, please contact Freeborn attorney Joel Bruckman at (312) 360-6461 or jbruckman@freeborn.com.

Freeborn

ABOUT THE AUTHOR

Joel B. Bruckman

Attorney

Chicago Office
(312) 360-6461

jbruckman@freeborn.com

Joel is an Associate in the Litigation Practice Group and a member of the Insurance/Reinsurance Industry Team and the Emerging Industries Team. He has extensive experience in White-Collar criminal investigations and post-indictment matters including allegations of Fraud, Theft, Embezzlement, Money Laundering and Anti-Trust Violations under The Sherman Act, Wire Fraud and private-sector Honest Services Fraud. As a former member of the FBI's Cyber Crimes Task Force during his time as a prosecutor for the Cook County State's Attorney's Office, Joel regularly advises clients on data security incident response strategies and best practices, from initial discovery and computer forensics investigations through statutory / regulatory notification compliance and subsequent government investigation and private-party litigation.

130+ Attorneys.
5 Offices.

Freeborn & Peters LLP is a full-service law firm with international capabilities and offices in Chicago, Ill.; New York, Ny; Richmond, Va.; Springfield, Ill.; and Tampa, Fla. Freeborn is always looking ahead and seeking to find better ways to serve its clients. It takes a proactive approach to ensure its clients are more informed, prepared and able to achieve greater success – not just now, but also in the future. While the firm serves clients across a very broad range of sectors, it has also pioneered an interdisciplinary approach that serves the specific needs of targeted industries.

Freeborn's major achievements in litigation are reflective of the firm's significant growth over the last several years and its established reputation as a Litigation Powerhouse®. Freeborn has one of the largest litigation departments among full-service firms of its size – currently with more than 90 litigators, which represents about two-thirds of the firm's lawyers.

Freeborn is a firm that genuinely lives up to its core values of integrity, effectiveness, teamwork, caring and commitment, and embodies them through high standards of client service and responsive action. Its lawyers build close and lasting relationships with clients and are driven to help them achieve their legal and business objectives.

For more information visit: www.freeborn.com

CHICAGO
311 South Wacker Drive
Suite 3000
Chicago, IL 60606
(312) 360-6000
(312) 360-6520 fax

NEW YORK
1155 Avenue of the Americas
26th Floor
New York, NY 10036
(212) 218-8760
(212) 218-8761 fax

SPRINGFIELD
217 East Monroe Street
Suite 202
Springfield, IL 62701
(217) 535-1060
(217) 535-1069 fax

RICHMOND
901 East Byrd Street
Suite 950
Richmond, VA 23219
(804) 644-1300
(804) 644-1354 fax

TAMPA
1 Tampa City Center
201 North Franklin Street
Suite 3550
Tampa, FL 33602
(813) 488-2920