Armstrong Teasdale

December 14, 2021 • Advisory • www.atllp.com

RESPONDING TO THE LOG4J CYBERSECURITY VULNERABILITY

Since last December, cybersecurity attacks on supply chain technologies that control and process personal and sensitive information for millions of corporations have intensified. Victims have included SolarWinds, Accellion, Microsoft and Kaseya, and tens of thousands of organizations that use their products and services.

Last Friday, a critical vulnerability – Log4j – was discovered in an application widely used in many software products. The early indications are that potential ramifications could be far-reaching. IT teams for major software companies have been working feverishly to patch vulnerabilities.

WHAT HAPPENED?

On Saturday, the director of the Cybersecurity and Infrastructure Security Agency (CISA), Jen Easterly, issued a call to action about the Log4j vulnerability:

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. End users will be reliant on their vendors, and the vendor community must immediately identify, mitigate, and patch the wide array of products using this software.

Although the vulnerability was first publicly disclosed on Friday, attacks exploiting the vulnerability started two weeks ago, according to Cisco and Cloudfare. Many technical explanations for the vulnerability have emerged, including theories from the Swiss government and a well-informed information sharing and analysis center for the health care industry, Health-ISAC.

WHAT DOES IT MEAN?

The Log4j exploit not only enables threat actors to remotely access corporate networks to obtain personal and sensitive information, but even worse, it enables threat actors to develop back doors to maintain access even after patches to the vulnerability have been deployed.

WHAT SHOULD ORGANIZATIONS DO?

CISA, Health-ISAC and the Apache Foundation have all issued guidance. From a

PEOPLE

Jeffrey Schultz, CIPP/US

SERVICES AND INDUSTRIES

Data Innovation, Security and Privacy

legal standpoint, we have already seen numerous instances this year where technology companies have been sued for, essentially, "knowing better how to secure against such vulnerabilities and not."

For example, a class action filed in Northern California against Accellion, a software company, alleges that Accellion breached numerous duties it owed to customers and users, including a fundamental duty of care:

1. Businesses whose systems and products are designed and marketed for the purposes of storing and transferring sensitive, personally identifying information ("PII") and personal medical information ("PMI") owe a duty of reasonable care to the individuals to whom that data relates.

As noted throughout this year, despite the broad and seemingly unwieldy patchwork of laws, regulations and industry standards that have arisen to address cybersecurity, "common threads" have emerged that, if followed, can reduce legal exposure, including:

- Written Information Security Programs (WISPs) that include patch and vendor management programs;
- Risk Assessments (RA) performed periodically, and the request for risk assessment information from vendors and service providers; and
- Incident Response Plans (IRPs) that address supply chain cybersecurity incidents.

Training employees and ensuring vendors and service providers have an updated WISP, RA and IRP not only assist organizations with technical risks but also risk management and legal risks.