BROOKLYN SOLUTIONS

LOG4J VULNERABILITY:

Reducing Risk Against Cybersecurity Threats To The Supply Chain

OVERVIEW

- Protected a large retailer against a severe supply chain vulnerability
- E-Meet capabilities and intelligent surveys enabled the customer to rapidly contact their suppliers at scale
- Customer established and maintained a 'fit-for-audit' stage
- **Successfully contacted 492 suppliers in just 72 hours**
- Implemented a risk strategy for future cybersecurity threats

The Challenge

The highest number of supply chain attacks of 2021 took place in December, with one of the most detrimental being the Log4j vulnerability. Commonly used by apps and services across the internet, Log4j is an open sourced logging library within a development language called Java. The vulnerability meant that threat actors had the ability to remote execute code and take control of anything that was making use of its components. The attack required very little expertise to execute, making Log4j one of the most severe vulnerability seen in recent years. Left unresolved, attackers could break into systems, steal sensitive data and infect networks with malicious software. A significant danger of these attacks was their ability to go undetected for months. Consequences for an organisation or it's third-parties suffering an attack would range from operational delays to corporate or government surveillance, including the potential loss of data.

Companies across most industries had to undergo a number of processes in order to assess whether any of their systems were vulnerable. They had begun with checking whether their own systems used Java, and if so, whether these systems were internet facing, which would make them more accessible to exploitation. After this activity commenced a mass-coordination event in which organisations were advised to contact all of their suppliers to assess their vulnerability. At Brooklyn Solutions, most of our clients have thousands of suppliers whom they had to rapidly assess on scale and on mass.

The Solution

Brooklyn's Step by Step Process

One of our clients, a major retail firm, was made aware of Log4j and its potential risk to hundreds of suppliers. Using Brooklyn, this client rapidly remediated risk from the Log4j vulnerabilities for the wider vendor tail, where it's suggested that over 60% of technology suppliers use Log4j as an indirect dependency. The Brooklyn platform fast-tracked a vendor consolidation exercise that would have usually required vendor managers to separately contact each supplier, as well as follow up on their individual responses. For our clients that were vulnerable to the cyberthreat, Brooklyn executed the following:
(1) Bespoke Cyberthreat survey template for Log4j, (2) Implemented a deadline & automated reminders, (3) Identified survey recipients, (4) Risk record created from negative responses, (5) Progress tracked by survey report.

Rapid Scalability
Gathered intel on the customer's suppliers and measures they have taken against the vulnerability, mitigating potential risk to the supplier's ability to provide their services securely

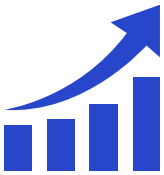
Auto-generated Risk Tracking
Our platform digitised and scaled response versus action by dividing auto-generated risk tracking, based on the responses from over 90 key suppliers. Vendors reported at risk were tracked and set-up with automated cadence.

Fit-For-Audit
Brooklyn ensured that our clients were digitally "Fit-ForAudit" by timestamping vendor submissions, in turn driving best practices of digital collaboration and customer-supplier transparency.

The Statistics

All suppliers managed by Brooklyn have up-to-date contact details that are periodically validated. With this built-in functionality as well as Brooklyn's E-Meet Capability, our client successfully determined that none of its systems nor its 3rd parties' had been exploited by the Log4j vulnerability.

Contacted 492 suppliers in 72 hours



10x more efficient than manual processes of vendor consolidation

Detected 6 suppliers vulnerable to an attack in the supply chain

Future CyberSecurity Risks

Despite the events of Log4j having occurred 6 months ago, experts warn that it remains a serious threat.

A new report by Rezilion has revealed that even at the end of April, almost 40% are still downloading vulnerable versions of the Log4j library. Even more troubling is that 60% of 17,840 open-source packages that use Log4j are still vulnerable and are yet to upgrade to the fixed version. Unfortunately, vulnerability exploitations of the supply chain will only continue to increase since the Log4j event . Threat actors have advanced their tactics, as they now lay low within networks that they have broken into, waiting for the opportunity to target high value data. It remains essential that businesses build defences against future attacks by establishing risk management at an early stage. Businesses cannot afford to simply assume that their web servers are safe.

With Brooklyn's automated e-meet capabilities, businesses can convert their post-breach strategy into a continuous identification of risk amongst third parties.

Deal Signed - Time to Deliver!

Brooklyn empowers the people managing customers or suppliers to digitise, strengthen, and automate contract delivery and risk management, with 7-10x ROI in the first year.

Brooklyn has a same-day onboarding experience.

Double your productivity within three months on Brooklyn's unified platform, supported by a network of transformation experts and delivery partners.

Do you want to protect your organisation from future cybersecurity threats? Request a demo or get in touch with our team of experts