CYCOGNITO

REPORT

Risky Business: Enterprises Can't Shake Log4j

EXECUTIVE SUMMARY:

Despite eradication efforts, Log4j continues to haunt large corporations eight months after the critical vulnerability was discovered.

Introduction

In December 2021 security teams scrambled to find Log4j-vulnerable assets and patch them. Eight months later many Global 2000 firms are still fighting to mitigate the digital assets and business risks associated with Log4j. The ease of Log4j vulnerability exploitation coupled with the critical nature of the bug, which allows attackers to run arbitrary code inside cloud and company networks, is driving a business-risk imperative to find vulnerable assets and patch them fast.

An examination by CyCognito of large enterprise external attack surfaces found 70% of firms that previously addressed Log4j in their attack surface are still struggling to patch Log4j-vulnerable assets and prevent new instances of Log4j from resurfacing within their IT stack.

Our research highlights business continuity risks such as digital asset sprawl, subsidiary risk and the importance of reducing the time it takes to identify a vulnerable Log4j asset and patch it.

Log4j: Analysis of Current and Lasting Legacy

On Dec. 9, 2021 the Log4j critical vulnerability (CVE-2021-44228) was first identified and was assigned a severity rating of 10 out of 10. It is a remote code execution class flaw found in the Apache Log4j library (part of the Apache Logging Project). This Log4j vulnerability is considered extremely dangerous because it is easy to exploit and soon after its discovery a public proof-of-concept became available.

Eight months later, Log4j has proven to be one of the worst vulnerabilities of the last few years, if not decade.

A July report (PDF) by the U.S. Department of Homeland Security stated: "The Log4j event is not over. Log4j remains deeply embedded in systems, and even within the short period available for our review, community stakeholders have identified new compromises, new threat actors, and new learnings."

Report Highlights

Our exclusive analysis of Log4j examines the external attack surfaces of three dozen Global 2000 companies, securely protected by CyCognito solutions. This report underscores the Log4j cybersecurity risks facing non-CyCognito customers and the at large cybersecurity community.

Incidents of vulnerable Log4j assets discovered by the CyCognito platform are based on simulated adversarial scans of exposed assets in the wild. These instances of Log4j (now mitigated) represented briefly exposed assets that, if overlooked, could have allowed an attacker access to the cloud or on-premises assets and networks of these organizations.

Top Log4j Takeaways for July 2022:

- Instances of Log4j-vulnerable assets are growing, not shrinking within a subset of companies examined.
- Some firms are seeing a doubling of Log4j-vulnerable digital assets within their external attack surface - not a decrease.
- Only 30% of firms with at least one past Log4j issue had no Log4j-vulnerable assets at the time of our analysis.
- Of those exposed Log4j-vulnerable assets, the most common were web applications.

Drilling Down on Data Points

Growing not Shrinking: After eradicating an external attack surface of Log4j-vulnerable digital assets, new instances of Log4j-vulnerable systems have come back online.

Of those firms with at least one Log4j vulnerability discovered in January 2022, 62% continued to report one or more Log4j-vulnerable assets exposed in July. Research did not indicate whether those were new or existing exposures.

Of the firms that did have an exposed asset in July, 38% experienced a gain of one or more Log4j-vulnerable assets. Data indicates that, for many companies, instances of new Log4j exposed assets remains a growing problem.

Double the Log4j Trouble: An examination of organizations revealed 21% of those with vulnerable assets in July experienced a triple-digit percentage growth in the number of exposed Log4j-vulnerable assets compared to January.

While the initial number of vulnerable assets were small within each organization examined, over a half-dozen are seeing a steady increase in the number of Log4j-vulnerable assets. One firm, with seven exposed assets in February of 2022 had 39 exposed assets in July.

Success Rates Rare: The number of organizations that experienced a drop in vulnerable assets was 38%. In each of those instances, CyCognito found zero instances of Log4J in their internet exposed attack surface in July.

Thirty-four percent of those firms with over one vulnerable asset in January had the same number of assets exposed in July.

Web App Worries: Breaking down the numbers even more, data reveals those firms with vulnerable assets had a greater number of web applications vulnerable to a Log4j exploit versus other types of systems.

This is concerning given web apps are high risk for business and their users alike because they often access or contain sensitive financial, confidential, or personally identifiable information.

Why Businesses are Struggling to Quash Log4j

A CyCognito analysis of why companies are struggling to squelch Log4j vulnerabilities once and for all are multifold.

First, organizations have underestimated the deep-rooted prevalence of Log4j software, and software vendors have not yet rid their products of the vulnerable Log4j code. The battle to mitigate Log4j-vulnerable assets is exacerbated by new instances of exploitable Log4j being introduced to an attack surface.

Further driving this trend is attack surface sprawl, subsidiary and business-unit risk, mergers and acquisitions (M&A) and a lag in the time to remediate vulnerabilities (known as mean-time-to-remediate, or MTTR).

CyCognito found that among Global 2000 companies, M&A activity is growing or shrinking an organization's attack surface by 5.5% each month (PDF). Organizations were initially unaware of 10-to-30% of their subsidiaries, according to separate CyCognito research published in June.

(See related CyCognito June report: "Anybody Got a Map?")

The global consultancy Bain & Company reports that M&A activity in 2022 is likely to reach US$4.7 trillion in deal value, making it the second-largest year on record. That kind of business change combined with emergent risks and poor IT ecosystem visibility make it extremely difficult for security and IT managers to have a 360-degree view of their entire external attack surface. This increases the odds of security gaps in their attack surface going unseen, opening them up to dangerous and preventable risks such as Log4j.

Why a Focus on Risk, Versus Vulnerability, is Paramount to Log4j Exposures

Trends in the growth of external attack surface sprawl are making it harder for security teams to reduce the mean time to remediate vulnerabilities – including Log4j.

In June 2021, the average time to fix a high-risk application vulnerability was estimated at 246 days (8.2 months), soaring from 194 days (6.5 months) at the start of that year, according to a study from Synopsys.

A CyCognito-sponsored research report by Informa Tech found security teams are suffering from cybersecurity debt issues. That's when new cybersecurity issues outpace a security teams' ability to mitigate existing ones.

Compounding the problem is inadequate and incomplete security scanning of external attack surfaces for vulnerabilities and other risks. CyCognito found competing discovery tools can leave between 10-to-50% of digital assets undiscovered and therefore untested and ignored.

Informa Tech found the majority of security teams only have the bandwidth to remediate about 50 vulnerabilities in an average month. Considering the deluge of new vulnerabilities discovered each month, current remediation rates are insufficient to keep pace with high and critical risk vulnerabilities such as Log4j issues.

That's why CyCognito advocates a business-risk-first management approach to cybersecurity that focuses on identifying and addressing the most urgent risks (such as Log4j) immediately within an attack surface.

CyCognito can help organizations find and remediate Log4j business risks with its unmatched ability to continuously discover the external attack surfaces of its customers using advanced AI-based techniques. Using simulated adversarial tactics, techniques and procedures, CyCognito automates an advanced attacker's reconnaissance efforts. It pairs an organization's internal vulnerability data with external threat intelligence to help organizations identify their most vulnerable and valuable assets so they can mitigate threats as they surface as close to in real time as possible.

About CyCognito

We are CyCognito, a revolutionary new approach to external cyber risk management driven to create positive business impact. Far deeper than external attack surface management, our platform helps organizations identify, understand and master their risk in profound new ways.

Fully-automated, highly scalable, and designed to function as promised, our platform uses advanced machine learning and natural language processing to allow for unprecedented reach, speed and accuracy. We can step into the shoes of potential attackers—which in turn helps us identify and secure gaps better than anyone. We help teams secure their attack surface by helping them determine true risks, where they need to focus and how they should invest. And then we use what we learn to help bridge cyber risk remediation across departments unlike ever before.

We are committed to helping you Rule Your Risk™. Learn more about the CyCognito platform.

To learn how the CyCognito platform uniquely helps you identify and prioritize the paths of least resistance into your IT ecosystem, so that you can eliminate them, visit **cycognito.com**.

CYCOGNITO