Accenture Cybersecurity Forum

Threat & Operations

Responding to Log4J: What Have We Learned? Where to from Here?

The Accenture Cybersecurity Forum (ACF) Threat and Operations Community convened a virtual roundtable, “Responding to Log4J: What Have We Learned? Where to from Here?” on February 17, 2022.

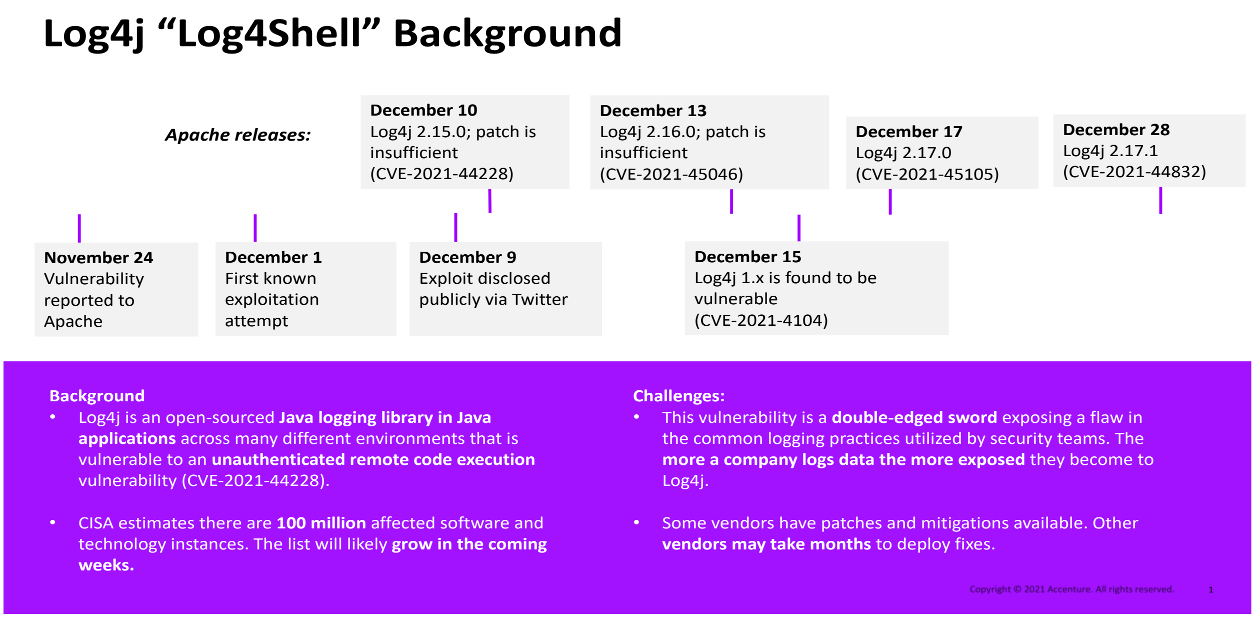
During this roundtable, Accenture subject-matter experts joined Community members to review lessons learned, best practices and concrete actions enterprises can take to remediate zero-day vulnerabilities such as Log4j.

The roundtable was conducted under the Chatham House Rule: ACF Threat & Operations Community members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers, nor participants, is revealed.

Below is a brief summary of the call:

The sudden impact of the Log4j vulnerability

“This is one of the worst incidents I’ve seen in my 20-year career,” said a subject-matter expert. The SME warned that many enterprises may be infected but unaware of its presence. “Attacks are easy from the threat actor perspective but it’s very difficult for enterprises to identify attack streams, because these attacks are outside the realm of normal network scanning tools.”



Log4j "Log4Shell" Background

Apache releases:

November 24 Vulnerability reported to Apache

December 1 First known exploitation attempt

December 9 Exploit disclosed publicly via Twitter

December 10 Log4j 2.15.0; patch is insufficient (CVE-2021-44228)

December 13 Log4j 2.16.0; patch is insufficient (CVE-2021-45046)

December 15 Log4j 1.x is found to be vulnerable (CVE-2021-4104)

December 17 Log4j 2.17.0 (CVE-2021-45105)

December 28 Log4j 2.17.1 (CVE-2021-44832)

Background

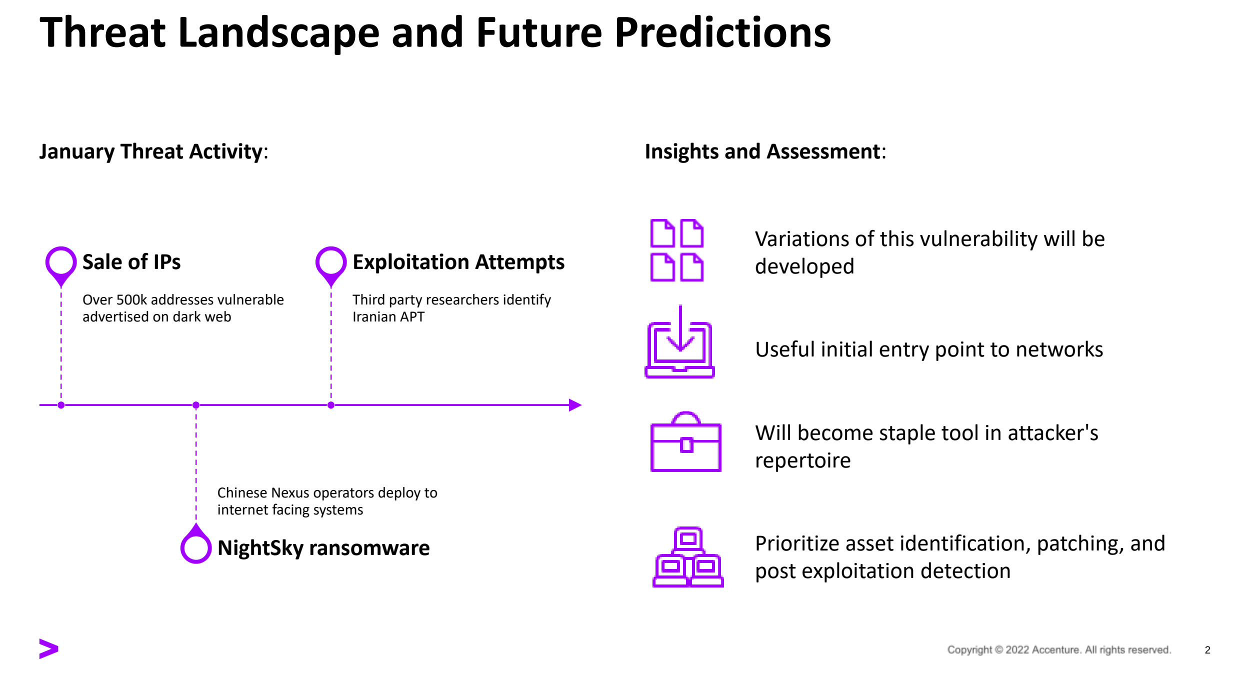
- Log4j is an open-sourced **Java logging library in Java applications** across many different environments that is vulnerable to an **unauthenticated remote code execution** vulnerability (CVE-2021-44228).
- CISA estimates there are **100 million** affected software and technology instances. The list will likely **grow in the coming weeks.**

Challenges:

- This vulnerability is a **double-edged sword** exposing a flaw in the common logging practices utilized by security teams. The **more a company logs data the more exposed** they become to Log4j.
- Some vendors have patches and mitigations available. Other **vendors may take months** to deploy fixes.

Threat activity today and tomorrow

Exploitation of zero-day vulnerabilities is becoming a standard weapon in the threat actor toolkit, said a subject-matter expert. Threat actors are leveraging the Log4j vulnerability as an initial point of entry into thousands of networks. "Hunting for a threat actor's presence is difficult because they can go deep into the enterprise environment and wait unseen for the right opportunity to attack," a subject-matter expert said.



Threat Landscape and Future Predictions

January Threat Activity:

Sale of IPs

Over 500k addresses vulnerable advertised on dark web

Exploitation Attempts

Third party researchers identify Iranian APT

Chinese Nexus operators deploy to internet facing systems

NightSky ransomware

Insights and Assessment:

Variations of this vulnerability will be developed

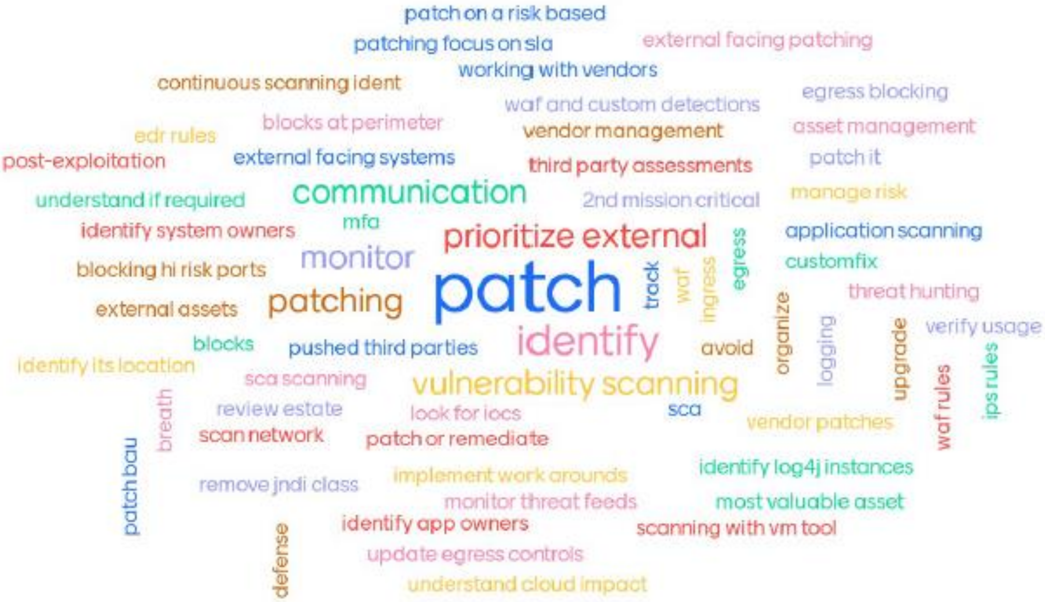
Useful initial entry point to networks

Will become staple tool in attacker's repertoire

Prioritize asset identification, patching, and post exploitation detection

Polling Question: What are the priority steps you have taken to remediate or mitigate Log4j-related risk?

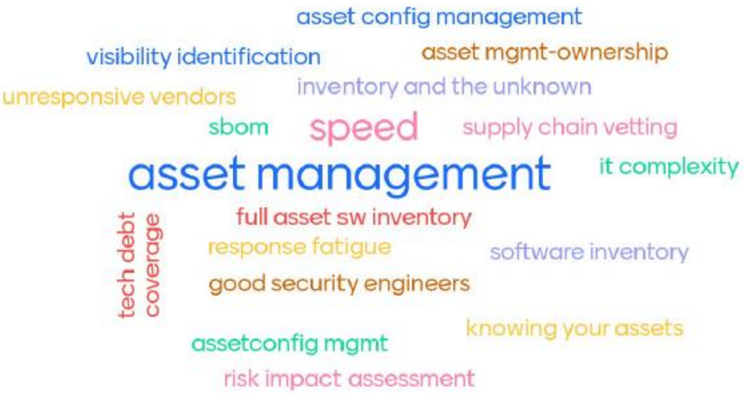
Patching in general, threat hunting & monitoring, vulnerability scanning and other processes to prioritize remediation efforts are clearly top of mind among Community members, according to their responses to a polling question.



One member noted they were surprised to see patching so prevalent on the list, echoing an SME's earlier statement about the lack of available patches for internal or niche systems, "[Patching] is very challenging especially in an environment like ours where we have a lot of different areas and systems … There's not just one patch that works for all 15 versions we use."

Polling Question: What is the most significant challenge ahead of us resolving the Log4j vulnerability and future zero-day vulnerabilities?

When asked about the most significant challenge they face in managing zero-day vulnerabilities, Community members acknowledge the value of greater visibility into their IT assets. As one said, "We're constantly in a race with our adversaries, and we're always starting from behind."



Valuable tools for improving visibility into enterprise IT and OT assets include:

- Software Composition Analysis (SCA)—Used to identify vulnerabilities in third party libraries used by applications. SCA scan reports can quickly identify which libraries contain Log4j vulnerabilities and give recommendations on which are fully safe versions.
- Dynamic Application Security Testing (DAST)—Used to identify vulnerabilities by running unauthenticated and authenticated scans on public-facing web applications.
- Static Application Security Testing (SAST)—Used to identify vulnerabilities in first party application code. While not a commonly used practice, it can be effective at enterprises that have not yet implemented SCA scanning as a best practice.

Strategic implications of zero-day vulnerabilities

Community members and subject-matter experts said that Log4j has underscored important strategic considerations:

- **C-level support**—“Management needs to understand what the bad guys are doing, and how it can materially impact the enterprise,” said a Community member. “Once they appreciate the risk, you can skip the debate about why cyber investments are necessary and move on to a discussion about how you intend to defend critical assets.”

  Another member added: “Operational technology is equated with safety, which is widely recognized as critical. Cybersecurity needs to be held with the same high priority.”
- **Cybersecurity governance**—Enterprises need a rigorous, consistent approach in managing relationships with third parties, any of which might be capable of introducing vulnerabilities into the enterprise. Internally, developer teams need to adopt sound hygiene practices.
- **M&A strategy**—The threat of inherited risk is heightened by zero-day vulnerabilities, and this will only increase over time as variants emerge from nation states and other threat actors. “You must make sure that the M&A team is not operating in a silo,” said a Community member. “Cybersecurity has to be part of the discussion.”
- **Talent & retention**—The community acknowledged that zero-day vulnerabilities can put severe strain on cybersecurity teams. One subject-matter expert knew of an enterprise that issued “Log4j Hero” certificates for going beyond the call of duty. “But now we’re always going beyond the call of duty and it’s just exhausting. It’s important that we find ways to keep giving them energy by, for example, offering more flexible work arrangements between crises.”

Leading practices

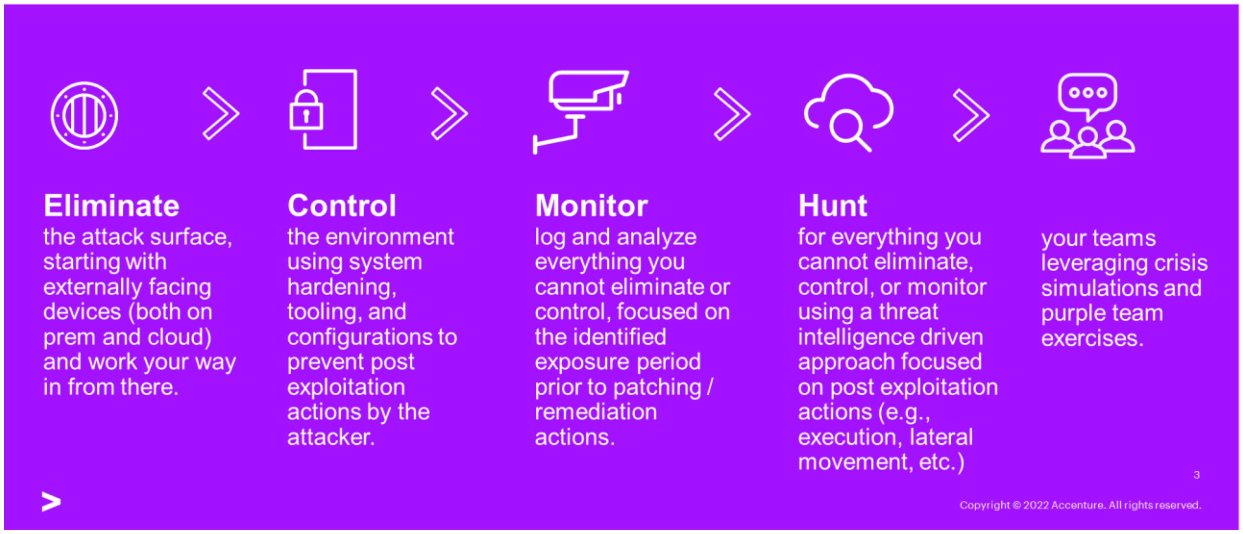
The following insights and recommendations were also shared:

- **“Be brilliant at the basics”**—"Threat detection, endpoint protection and multi-factor authentication aren’t sexy. They aren’t fun,” said a Community member. “But they are critical.”

A subject-matter expert added: “We can’t always predict what the next zero-day may be, but there are things we can do proactively in terms of network hygiene and security: asset management, network segmentation, two-factor authentication and egress filtering, making sure that the traffic leaving your network is going to a legitimate destination.” Another subject matter expert added: “Egress filtering is important because the number one thing that frustrates an attacker is not being able to connect back out of your network.”

- **Understand the threats**—Threat intelligence and a deep understanding of enterprise assets can help set security investment priorities. “It’s important to know what you look like to your adversaries and to know your high-value assets and programs,” said a subject-matter expert. “The nexus of what’s important to the business and what threat actors want to compromise is a really good place to start from a prioritization standpoint.”
- **Embrace the trend toward a software bill of materials (SBOM)**—"We expect people will be asking their vendors to provide a SBOM, and that will be incredibly valuable as long as people are using that information and cataloging it properly,” said a subject-matter expert. Others noted a need to adjust or reconsider usage of open-source libraries. Several community members stressed the importance of software composition analysis.
- **Devote 5% of your attention externally**—Look for opportunities to collaborate within your industry, technical community or country to strengthen cybersecurity at a macro level. One member suggested more engagement with the open-source community, such as underwriting project development.

Breach Readiness and Response



Eliminate the attack surface, starting with externally facing devices (both on prem and cloud) and work your way in from there.

Control the environment using system hardening, tooling, and configurations to prevent post exploitation actions by the attacker.

Monitor log and analyze everything you cannot eliminate or control, focused on the identified exposure period prior to patching / remediation actions.

Hunt for everything you cannot eliminate, control, or monitor using a threat intelligence driven approach focused on post exploitation actions (e.g., execution, lateral movement, etc.)

your teams leveraging crisis simulations and purple team exercises.

3

On behalf of the Accenture Cybersecurity Forum Threat and Operations Community, we thank our subject matter experts and those of you who were able to join the roundtable for your valuable contributions.

Josh Ray
Accenture Managing Director — Global Cyber Defense Lead
Accenture Cybersecurity Forum Threat and Operations Community Chair
LinkedIn

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 674,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at accenture.com.

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us on @AccentureSecure on Twitter or visit us at www.accenture.com/security.

View the entire suite of ACF roundtable summaries on our webpage – here.