The FTC means business when it comes to pushing organizations to patch Log4j promptly. On January 4, 2022, the FTC blog issued a reminder that failure to mitigate known software vulnerabilities could result in legal action.

The FTC highlighted the $700 million fine issued to Equifax for its failure to patch a known vulnerability – which resulted in exposing the personal information of 147 million consumers – as proof that they are holding businesses accountable for security.

In addition to the punitive and legal risks faced from the Log4j vulnerability, there is clear evidence that threat actors, including known nation-state actors and cybercrime organizations, have moved quickly to exploit "Log4Shell."

The exploit makes it simple to execute malicious code remotely, and is estimated to affect hundreds of millions of devices. In parallel, enterprises, vendors and cloud services have moved to patch their systems fairly swiftly.

But given its pervasiveness, finding every single instance of Log4j in every environment could take years. And every day a vulnerable device goes unpatched is another day that an attacker could compromise a system, install a backdoor, and quietly wait to attack.

Why Log4Shell is Hard to Find

Even if you've taken the initial steps to patch your systems, the problem is that Log4Shell is not your typical vulnerability. Log4j is not software from a single vendor.

The Apache Log4j software library is an open-source building block used widely across millions of web sites and cloud applications you use, adapted in different ways. It's also used in a range of operational tools, equipment and devices you may never have imagined were running so much code. In some instances, it's even repackaged, renamed, and/or embedded into the application itself — so deeply buried that it is difficult to find.

The Tanium Advantage in Surfacing and Remediating Log4Shell

Finding which assets across your environment need to be updated is challenging. Many endpoint tools can't scan all your workloads at scale or provide accurate answers about what's running on your network quickly enough. When it comes to addressing your cyber security challenges, the Tanium platform has an advantage with speed and accuracy, and delivers valuable endpoint visibility and control using a combination of tools:

- Tanium Reveal enables you to find and review sensitive data by inspecting the contents of user and system files. Quickly search JAR, EAR, WAR, and ZIP files of vulnerable usage of the Log4j library, including those repackaged by third-party vendors.

- Tanium Threat Response allows you to investigate and hunt for vulnerable jar files by hash, file name, and versions. In addition, you can alert your SOC team of any signs of exploitation by importing the relevant Yara rules, IOCs, and SIGNALs to scan for the malicious Log4j payloads. Then take immediate action to quarantine, download logs, collect evidence or quickly pivot and search for forensic artifacts at scale across your enterprise.

- Tanium Comply provides executive and actionable reporting and vulnerability assessments of all Common Vulnerabilities and Exposures (CVE)s including the Log4J vulnerability CVE-2021-44228.

- Tanium Patch and Deploy allows you to quickly remediate at scale and deliver updated versions of software you've identified as vulnerable.

In addition to the tools and technology, the Tanium User Community is where you can engage with industry peers and other security experts to get technical guidance on Tanium products. Contributors from the Tanium community provide insights and updates on major threats and have been a valuable resource for technical details on the Log4Shell vulnerability.

Adding Chuco Security Services to Your Defenses

At Chuco, we've already been helping many of our clients – from large enterprises to smaller organizations – in finding, patching and remediating Log4j vulnerabilities. Our Tanium Consultants, many of whom have previously worked at Tanium and/or on enterprise SecOps teams, are all Tanium Certified and can help with getting the most out of Tanium to address your needs.

- Configuration & Planning: From configuring Tanium Reveal and Threat Response to identifying and patching Log4j, we can work with you to take a structured approach to detection and mitigation. Chuco will collaborate with your experts to conduct assessments and determine how well your Tanium environment is performing, then work with you to build and deliver a roadmap to mature and maximize your investment in Tanium.

- Hands-On Support: When you need "all hands on deck" but can't afford to take your security analysts off other tasks, we have security experts who can augment your teams, bringing an understanding of business processes together with the "hands-on" technical expertise you need to execute your detection and mitigation plan.

- **Customizations:** Through automated features and robust APIs, the Tanium platform is known for its built-in extensibility. We can help you get the most out of Tanium by writing custom scripts, and configure Tanium to integrate with all your other critical enterprise SOC tools to streamline and orchestrate the most effective detection and response solution that fits your organization's needs.

- **Post-Exploitation Response:** Realistically, Log4j is so pervasive that not every device that is using it can be updated or patched, such as IOT devices or outdated appliances. It's paramount to work with an experienced team who understands the threats and vulnerabilities to your business and can maximize the coverage and capabilities of your security tools.

  If your organization has been exploited, we can help you leverage the rest of the Tanium security suite to respond at full capacity, including supporting your incident response operations by collecting forensics evidence, quarantining endpoints, and conduct deep dive investigations to tackle serious cybersecurity threats and issues.

Please get in touch to discuss how Chuco can help you with Log4j mitigation. Our consultants are standing by to help design or extend your response strategy, and put hands on keyboard to help execute.