Log4j/Log4Shell Security Team Response

Immediate assistance to discover if and where you may be vulnerable

On December 10th, 2021, a serious flaw was disclosed involving the widely used Java logging library Apache Log4j. This vulnerability has the potential to allow unauthenticated remote code execution (RCE) on nearly any machine using Log4j.

Catapult and other industry security leaders prepared a series of trustworthy scripts and utilities we can use within your Azure environment to rapidly detect your vulnerabilities and help you prioritize remediation efforts. **Our utilities quickly identify where you may be exposed and how extensive the remediation will be.** This offer does not cover the recovery of compromised systems.

HOW IT WORKS:

Once we have access to the client's tenant, Catapult's Security Response Team will:

- Run our scripts and tools to identify vulnerable, compromised, unpatched log4j devices
- Generate an inventory list of affected systems and prioritize areas to remediate
- Produce a basic report outlining extent of damage
- Deliver a high-level remediation plan to address patching, clean up of remediation items, and recommendations going forward

PRICE: $7,500

WHAT IS AFFECTED:

IMPACT: Arbitrary code execution as the user the parent process is running as: code fetched from the public internet; or lolbins already present on system; or fetching shared secrets or environment variables and returning them to the attacker.

TARGETS: Servers and clients that run Java and log anything using the log4j framework. It is primarily a server-side concern, but any vulnerable endpoint could be a target or pivot point.

DOWNSTREAM PROJECTS: Assume anything that includes log4j, like Elasticsearch, Apache Struts/Solr/Druid/Flink, etc., is affected in a way that requires mitigation.

AFFECTED VERSIONS: Log4j 2.x has been confirmed; log4j 1.x is affected only indirectly (previous information disclosure vulns, in some configurations).

APPLIANCES: Don't forget to check appliances that may be using Java server components, but will not be detected by unauthenticated vulnerability scanning.

LOG FORWARDING: Logging infrastructure often has many "northbound" (send my logs to someone) and "southbound" (receiving logs from someone) forwarding/relaying topologies. Chaining them together for exploitation must also be considered.

CLOUD: Though multiple large providers are also affected, this guide focuses on the customer-managed side.

WHY IT MATTERS:

It's not just your internal applications... another 2,000+ third-party applications have known vulnerability to this.

Experts say the flaw leaves hundreds of millions of systems vulnerable to attack. The head of the U.S. government's cybersecurity agency called this among the biggest threats she has seen in her career.

WHAT YOU CAN DO:

Even if you decide not to go with Catapult's Log4j/Log4shell Security Incident Response, you should:

1. **Check if you are impacted:** Any organization with assets running a version of Log4j above version 2.0 and below version 2.15.0 (the fixed version release) is impacted by the vulnerability.
2. **Review your most recent vulnerability scan results**, which contain the location of any Log4j installations active within the environment.
3. **Update to Log4j version 2.17.1** right away.
4. **Prioritize this threat stream:** Following CISA guidelines, you should ensure that you install a web application security system (WAF) with rules that automatically update so that your SOC (Security Operations Center) is able to concentrate on fewer alerts.

FOR MORE INFORMATION

- Current customers, please reach out to your **Customer Success Manager** or **Security Coach**
- For all other inquiries, contact the Security Response Team at **SRT@catapultsystems.com**