NYC Cyber Command

December 10th, 2021

Threat Intelligence Advisory

Widespread Exploitation of a Critical Apache Utility Vulnerability Likely in the Near-Term

TLP: Amber

Rating: High

Key Takeaway:

- NYC3 CTI assesses that a critical vulnerability (CVE-2021-44228) impacting the Apache Log4j2 utility (commonly referred to as Log4Shell) almost certainly affects assets the City operates as well as assets that City vendors operate.
- NYC3 CTI assesses that widespread exploitation of this vulnerability is very likely to be observed in the near-term.
- NYC3 Vulnerability Management on 10 December 2021 sent a Citywide notification (NYC21-0306 APACHE LOG4J ZERO-DAY VULNERABILITY) with details and guidance on mitigating CVE-2021-44228.
- NYC3 CTI recommends agencies conduct retrospective investigations on the shared indicators within your environment (see links below) and conduct monitoring for these indicators until patching is complete.

Summary and Details of Advisory:

Background

Between late November and early December 2021, a critical vulnerability (CVE-2021-44228) impacting the Apache Log4j2 utility was reported, resulting in several fixes and code revisions from the Apache Software Foundation. The Log4j2 utility is extensively used in numerous Apache Software Foundation products, and several security researchers and vetted intelligence partners as of 10 December 2021 had identified active exploitation of this vulnerability in the wild.

Assessment

NYC3 CTI assesses that a critical vulnerability (CVE-2021-44228) impacting the Apache Log4j2 utility (commonly referred to as Log4Shell) almost certainly affects assets the City operates as well as assets that City vendors operate. Log4j is a Java library utility that provides logging capabilities and is included with almost all enterprise products released by the Apache Software Foundation; Log4j has a near-ubiquitous presence in almost all major Java-based enterprise apps and servers.

- Log4j is included with almost all enterprise products released by the Apache Software Foundation, to include Apache Struts, Apache Flink, Apache Druid, Apache Flume, Apache Solr, Apache Flink, Apache Kafka, Apache Dubbo, and possibly many more.[1]

- Open-source projects like Redis, ElasticSearch, Elastic Logstash, the National Security Agency's Ghidra, and others also use Log4j in some capacity, and all companies that use any of these products are very likely also indirectly vulnerable to CVE-2021-44228 exploits.[2]

- Companies with servers vulnerable to CVE-2021-44228 likely include Apple, Amazon, Twitter, Cloudflare, Steam, Tencent, Baidu, DIDI, JD, NetEase, and possibly thousands more.[3]

NYC3 CTI assesses that widespread exploitation of CVE-2021-44228 is very likely to be observed in the near-term. CVE-2021-44228 is a Remote Code Execution (RCE) vulnerability that allows a threat actor to craft a special data packet that can eventually trigger remote code execution.

- Multiple cybersecurity firms as of 10 December had observed mass scanning activity from multiple hosts checking for servers using Apache Log4j.[4][5]

- The first proof-of-concept exploit for CVE-2021-44228 was published on GitHub on 9 December.[6]

- Multiple researchers and organizations as of 10 December claimed to have observed attempts to exploit CVE-2021-44228 in honeypot environments, according to vetted intelligence partner reporting. The same vetting intelligence partner observed ongoing opportunistic attempts to exploit this vulnerability.

- An independent security researcher as of 10 December claimed to have observed threat actors deploying cryptominers by exploiting CVE-2021-44228.[7]

Existing Defenses For DoITT Environment and Managed Agencies:

- None.

Proactive Steps Taken:

- NYC3 Vulnerability Management on 10 December 2021 sent a Citywide notification (NYC21-0306 APACHE LOG4J ZERO-DAY VULNERABILITY) with details and guidance on mitigating CVE-2021-44228.

[1] Recorded Future | Log4j zero-day gets security fix | 10 December 2021
[2] Recorded Future | Log4j zero-day gets security fix | 10 December 2021
[3] YfryTchsGD | GitHub | 10 December 2021
[4] Greynoise | Twitter Feed | 9 December 2021
[5] Bad Packets | Twitter Feed | 10 December 2021
[6] Tangxiaofeng7 | GitHub | 9 December 2021
[7] Omri Segev Moyal | Twitter Feed | 10 December 2021

- Log-based detections associated with the vulnerability are being incorporated into the City's security controls and will be updated pending additional detections.

Recommendations:

- NYC3 CTI recommends agencies conduct retrospective investigations on the shared indicators (gist links) within your environment and conduct monitoring for these indicators until patching is complete.
  - https://gist.github.com/Neo23x0/e4c8b03ff8cdf1fa63b7d15db6e3860b
  - https://gist.github.com/gnremy/c546c7911d5f876f263309d7161a7217
  - https://gist.github.com/superducktoes/9b742f7b44c71b4a0d19790228ce85d8
- Agencies are advised to update the Apache Log4j-2 to version Log4j-2.15.0 or greater.
- After appropriate testing, agencies that cannot upgrade to Log4j-2.15.0 can mitigate exposure by:
  - Users of Log4j 2.10 or greater may add -Dlog4j.formatMsgNoLookups=true as a command line option or add log4j.formatMsgNoLookups=true to a log4j2.component.properties file on the classpath to prevent lookups in log event messages.
  - Users since Log4j 2.7 may specify %m{nolookups} in the PatternLayout configuration to prevent lookups in log event messages.
  - Remove the JndiLookup and JndiManager classes from the log4j-core jar. Removal of the JndiManager will cause the JndiContextSelector and JMSAppender to no longer function.

Sources

NYC3 CTI also incorporated information gathered from partners, vendors, and other vetted sources.