NYC Cyber Command

VULNERABILITY RATING // CRITICAL

NYC21-0306 APACHE LOG4J ZERO-DAY VULNERABILITY

NYC3 PUBLISHED: 12/10/2021

MITIGATION

Agencies are advised to update the Apache Log4j-2 to version Log4j-2.15.0 or greater. Apache has identified 1 Critical vulnerability affecting Log4j 2.0 through 2.14.1. For those users who cannot upgrade to 2.15.0, there is a temporary mItigation.

Some known vulnerable products are Apache Struts2, Apache Solr, Apache Druid, Apache Flink, various Cloud services as well as any Java based applications that utilize this logging library.

All patches and workarounds should be tested before implementation in the production environment. Critical vulnerabilities are required to be patched within 7 days, High vulnerabilities are required to be patched within 30 days, as per the NYC3 Citywide policy for vulnerability mitigation standard (S-DE-CM-02).

IMPACT SUMMARY

Apache identified a Remote Code Execution (RCE) Zero-day vulnerability, (CVE-2021-44228), in the popular Java logging library Log4j allowing an attacker to craft a special data packet that can eventually trigger a remote code execution.

Successful exploitation of these vulnerabilities can lead to a complete system compromise.

SOURCES + REFERENCES

https://www.lunasec.io/docs/blog/log4j-zero-day/
https://www.bleepingcomputer.com/news/security/new-zero-day-exploit-for-log4j-java-library-is-an-enterprise-nightmare/