12/14/2021

Log4j Zero-Day

12/16/2021 Update

- CyZen is aware and tracking vulnerability CVE-2021-45046 associated with the patch fixing the critical Log4j Zero-Day exploit. This new vulnerability is currently being exploited in the wild. It was found that the Apache Log4J 2.15.0 update was incomplete in certain non-default configurations. This flaw enabled attackers to perform denial-of-service attacks, as well as an information disclosure error that could expose sensitive data.
- It is recommended to update to Log4j 2.16.0 immediately.
- CyZen is currently tracking exploits in the wild and has updated our existing rules with new indicators.

Summary

Log4Shell is a critical severity vulnerability (CVE-2021-44228, CVSSv3 10.0) impacting multiple versions of the Apache Log4j 2 utility. It was disclosed publicly via the project's GitHub on December 9, 2021. This vulnerability, which was discovered by Chen Zhaojun of Alibaba Cloud Security Team, impacts Apache Log4j 2 versions 2.0 to 2.14.1. The vulnerability allows for unauthenticated remote code execution.

Log4j 2 is an open-source Java logging library developed by the Apache Foundation. It is widely used in many applications and is present, as a dependency, in many services. These include enterprise applications as well as numerous cloud services.

Important Details

- The Apache Software Foundation has issued an emergency security update to the Java library Log4j after a security researcher released proof-of-concept code and reports of active scanning for vulnerable servers.
- This vulnerability affects all versions from 2.0-beta9 to 2.14.1 with a severity score of 9.8 (critical) on the CVSSv3 severity scale and provides the threat actor with remote code capabilities.
- CVE-2021-44228 can be easily exploited, with little technical skill, if the "log4j2.format.MsgNoLookups" option in the library's configuration is set to "false".

Mitigations/Recommendations

- Organizations are highly encouraged to update Log4j to 2.15.0 as soon as possible.
- If an organization cannot update to 2.15.0 at this time, it is recommended that the organization set the value of "Log4j2.format.MsgNoLookups" to "true".

CyZen Detection

- CyZen has created a new static rule for Log4j exploit strings that have been observed in the wild.
- CyZen has enabled 2 new Advanced Analytics rules for known malicious external IPs associated with Log4j exploit.
- CyZen has performed manual searches for customers with high fidelity indicators of compromise.

Sources:

- Apache Software - https://nvd.nist.gov/vuln/detail/CVE-2021-44228
- Vulnerability Details - https://logging.apache.org/log4j/2.x/security.html