Security Advisory for Professional Services – Solutions

Critical vulnerability in Apache Log4j (Log4Shell, CVE-2021-44228)

Release Date: 2021-12-14 13:05:23
Last Update: 2021-12-14 15:26:30

Summary

Apache Log4j2 <= 2.14.1 has a JNDI feature that allows it to look up the contents of a log message by using a name, via the LDAP protocol. Unfortunately though, it doesn't protect against attacker-controlled LDAP endpoints, which means that if an attacker can control log messages (or log message parameters) they can trigger a lookup to a malicious LDAP server, and subsequent loading and execution of arbitrary Java code.

The vulnerability is rated critical with an initial CVSS3 score of 10. (NVD has not been assigned a score yet)

Details

Key Takeaways

Vulnerability is present in all applications embedding Log4j (ver. 2.0 to 2.14.1.) for audit logging feature. Mainly Apache stack but also applications like Elastic search, Redis, etc. Vulnerability based on forcing applications to log a specific string which forces vulnerable system to download and run malicious script from attacker-controlled domain. According to security researchers' apps and services across the globe has already been actively scanned for vulnerable versions of Log4j by malicious actors. Attack can be blocked with a config change and patch.

Affected Solutions

Confirmed affected solutions

- UC Integration Server (hot fix / workaround available)

The UC Integration Server includes the following applications:
UC Integration Launcher, UC Salesforce Integration.

Confirmed not affected solutions

- OSILA

(please consider “Support Note DirX-15 for CVE-2021-44228 ” as DirX is part of the solution)

- Solution Kit V3 / V3R1 (SK V3/V3.1)

- Professional Services – Solutions Framework V4 / V5 (PSSF V4/V5)

The solutions SK V3/V3.1 and PSSF V4/V4 include the following applications: Communication Desk, Communication Desk Web, AgentDesktop Web, Agent Realtime View Web, Integration Connector (JAVA / COM), Remote Agent, Reporter Package (Multisite Datacollector and WebScheduler), ACD Control, Dashboard, Name Provider Service, Realtime Board, SalesForce Adapter, SkillManagement and customized Concierge based on Solution Kit V3 and Professional Services – Solutions Framework V4 / V5.

Recommended Actions

General Recommendations:

- Focus on internet connected systems first
- Check whether system is running log4j version 2.0 to 2.14.1
- For non-Atos Unify products contact your system or software vendor to validate if log4j is in use and if any additional actions are required

For affected Atos Unify products

- Check whether a system may be compromised. To detect compromise, perform log check as following link
- If you have network monitoring tools in place implements suitable rules in order to detect potential attacks
- If you identify a system being compromised report it to the respective Security Officer or IT manager and consider disconnecting it from the network

References

Important links:

https://www.lunasec.io/docs/blog/log4j-zero-day/

https://github.com/lunasec-io/lunasec/blob/master/docs/blog/2021-12-09-log4j-zero-day.md

https://twitter.com/P0rZ9/status/1468949890571337731

https://logging.apache.org/log4j/2.x/download.html

https://github.com/Neo23x0/log4shell-detector

https://www.tenable.com/cve/CVE-2021-44228

https://supportcenter.us.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk176884

https://blog.netlab.360.com/threat-alert-log4j-vulnerability-has-been-adopted-by-two-linux-botnets