APACHE LOG4J ZERO DAY VULNERABILITY

Conscia Cyberdefense Threat Intelligence Flash Alert (UPDATE)

Version 1.2 (13.12.2021 09:45 CET)

EXECUTIVE SUMMARY

A serious and easily exploitable remote code execution (RCE) vulnerability (CVE-2021-44228) has been found in the Apache Log4j logging framework, which is embedded in many Java applications on servers, appliances, and clients. Consequences of this vulnerability include attacker control over the target environment.

*This update contains additional risk and mitigation guidelines presented in **bold**.*

DESCRIPTION

Apache Log4j2 JNDI (Java Naming and Directory Interface) versions prior to 2.15.0 contain a vulnerability, where an attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. A working exploit for the vulnerability has been published and Internet-wide scanning for vulnerable hosts is currently taking place by various threat actors.

Based on current knowledge, the vulnerability may have been exploited up to 9 days before its public disclosure.

RISK ASSESSMENT

Due to the issue's ability to compromise exposed systems without authentication, and with relative simplicity, the Conscia Cyberdefense team rates this event as **CRITICAL** RISK for all organizations using Java technology to support Internet-exposed business-critical processes, **who do not strictly filter egress network traffic**. **For organizations that strictly filter egress network traffic, we rate the this vulnerability as HIGH RISK.**

Note that this vulnerability is likely to be widespread in various software solutions and it may take a long time to completely eradicate it from most environments.

CONSCIA CYBERDEFENSE PROTECTION

For customers using Microsoft Defender for Endpoint, Palo Alto Cortex XDR, or Fidelis Endpoint security solutions, we have determined that these solutions now contain vendor rules for this vulnerability that provide its prevention and/or detection. Additionally, the Cyberdefense team has developed an additional, broader and better custom detection rule that is being deployed in your environments from Sunday night onwards. We are also threat hunting for known IOCs related to this vulnerability. As a result, we are able to detect exploitation of vulnerable hosts where these endpoint agents are installed.

SHORT-TERM CUSTOMER GUIDELINES

In the short term, we suggest that customers initially focus on all services exposed to untrusted users (Internet or other) using the following guidelines:

1. **Identify vulnerable or potentially vulnerable exposed systems using analysis of software or a network vulnerability testing tool. If unable, assume that hosts running Java-based web applications are vulnerable.**
2. **If possible, patch or reconfigure the log4j software to eliminate the vulnerability.**

3. **Configure strict egress network filtering between vulnerable or potentially vulnerable systems and external networks (typically Internet), where you block all traffic except to trusted external systems. Note that the vulnerability can use any port, and encrypted sessions, therefore application-specific filtering is a weak countermeasure. This remediation step alone will prevent the vast majority of exploitation options, and should be done even if other steps remediation steps have been taken.**
4. **If the vulnerable or potentially vulnerable system is running an EPP/EDR endpoint security agent mentioned above and is included in the Conscia Cyberdefense MDR services, exploitation will be prevented / detected and responded to.**
5. **If the vulnerable or potentially vulnerable system is NOT running an EPP/EDR endpoint security agent, work with the Conscia Cyberdefense team to onboard the host into the MDR service.**
6. **For exposed appliances that are not likely to accept EDR software or reconfiguration, work with the appliance vendors to determine remediation options. In the meantime, configure strict egress network filtering from appliances to external networks, if possible.**
7. **As the vulnerability has been exploited in the wild for at least 9 days before public disclosure, consider performing forensics on your most sensitive systems to ensure that they have not been compromised earlier.**

If you need assistance with any of these actions, you can engage the Conscia Cyberdefense incident response team via your dedicated security analyst or the Incident Response hotline (+386 1474 6555) to conduct deep system examination and forensics. Our engagement will be billed based on agreed IR hourly rates.

LONG-TERM CUSTOMER GUIDELINES

In the long term, customers must identify the presence of this vulnerability across their information system, in other packages exposed to the network, or locally allowing for privilege escalation.