Cisco Partner

Recommended Actions

Apache Log4j is a java-based logging framework library. The JNDI (Java Naming and Directory Interface) component in Apace Log4j versions 2.0-beta9 through 2.14.1 improperly handles log messages. Certain user-supplied log messages are improperly executed prior to being written to log files. Unauthenticated remote attackers can leverage specially crafted LDAP log messages to download and execute arbitrary code with elevated privileges. Please note that due to the widespread use of this library that other vectors besides LDAP are possible depending on the implementation.

There are several methods to detect evidence of exploitation in your environment using Cisco Security services:

Cisco Next Gen Firewalls with IPS (Threat Prevention)

- Cisco IPS receives new policy rules and signatures every two hours, so your security is always up to date. Cisco Talos leverages the world's largest threat detection network to bring security effectiveness to every Cisco security product. This industry-leading threat intelligence works as an early-warning system that constantly updates with new threats.
- Use Snort 2 rules 58722-58744, 58751 and Snort 3 rules 300055-300058 to block the log4j threat.
- Block outbound connections from your DMZ hosts on the LDAP port – 389/tcp
- Create a Correlation Rule that triggers for any 389/TCP connections initiated from DMZ hosts to anywhere. Add appropriate alerting to this rule to notify of potential compromise.
- Decryption needs to be enabled to ensure that all threats over HTTPS are also identified.
- Turn on auto updates to ensure the rule base is always up to date or manually update them daily.

Use SecureX

- SecureX is a cloud-native, built-in platform experience that connects the Cisco Secure portfolio and your infrastructure including 3rd party devices.
- Integrate 3rd party security threat feeds to enrich telemetry data from multiple sources to ensure accuracy
- Use the SOAR functionality inside SecureX to automate remedial actions such as domain blocking, device quarantine and isolation if a device is infected by Log4j.
- Use the inbuilt threat hunting tools to see if threats like Log4j are already present in the network. For a list of indicators of compromise (IoC) see: https://blog.talosintelligence.com/2021/12/apache-log4j-rce-vulnerability.html

Cisco Secure Network Analytics (SNA)

- SNA provides agentless advanced threat detection, accelerated threat response, and simplified network segmentation using multilayer machine learning and entity modelling. With advanced behavioural analytics, you will always know who is on your network and what they are doing.
- With SNA deployed you can combat Log4J via:
    - Searching for Past Evidence of Exploitation
    - Detect Future Malicious Communications
    - Log4j Detection with the Flow Sensor Payload Data
    - Search for Abnormally Large LDAP Queries

Cisco Secure Endpoint

- Secure Endpoint offers cloud-delivered, single agent, advanced endpoint detection and response solution to rapidly detect, contain, and remediate advanced threats.
- Rapidly identifies and protects against Log4j exploits in multiple ways. It blocks threats that try to exploit the Log4j vulnerability with multifaceted prevention techniques, including machine learning and behavioural protection. Furthermore, robust detection and response capabilities reduce dwell time. Finally, rich threat intelligence from the Cisco Talos security research team allows you to have the latest protection from attackers.
- Cloud IOC’s in Secure Endpoint have been updated to include new Log4j-related detections and new clamAV signatures are available to block attacks exploiting Log4j.
- In case any threats get through, advanced Endpoint Detection and Response (EDR) functionality such as SecureX Threat Hunting and Orbital Advanced Search quickly uncovers signs of Log4j exploitation attempts and post-exploitation activity such as

lateral movement, suspicious command launch and others. This includes two new Orbital queries that identify entities affected by the Log4j vulnerability on Windows and Linux devices (windows_log4j_monitoring and linux_log4j_monitoring).