Cyber Vulnerability Alert and Mitigation Resource – Log4j

December 2021

Cybersecurity Branch
Surface Operations, Security Operation
Transportation Security Administration (TSA)
Questions? Email: So-Cyber-Servicedesk@tsa.dhs.gov

Overview

The Transportation Security Administration (TSA) assesses the risk of a critical vulnerability being actively exploited in the U.S. Transportation Sub Sector[a] as HIGH.[b] We base this assessment on an evaluation of the likelihood and impact of malicious cyber actors actively using CVE-2021-44228 (NIST) across a large range of entities (CISA log4j guidance).

Vulnerability Summary

Malicious cyber actors[c] are actively attempting to exploit log4j. This is particularly concerning because it does not require significant capability to exploit this vulnerability and log4j is ubiquitous across industries, government agencies, and academia. It is expected that this vulnerability will evolve as persistent penetration methods are developed by threat actors. New tactics and subsequent techniques are likely to be observed to take advantage of the high exposure factor and trivial nature of exploitation of this vulnerability (Dragos). National security and the economy is dependent upon the U.S. Transportation Sub Sector's ability to deliver goods and services. This dependency makes this sector a potential target of malicious cyber actors.

The current Mitre ATT&CK Tactics and Techniques incorporating the log4j vulnerability into adversary activity are referenced in table 1 (not independently verified by TSA):

Table 1. MITRE ATT&CK

MITRE ATT&CK	
Reconnaissance	**Resource Development**
Mass scanning has been observed by organizations attempting to thumbprint vulnerable systems. (Microsoft, Palo Alto)	Proof of concepts have been developed for exploiting the Log4j vulnerability and further development will likely continue. (Nozomi, Microsoft)
Initial Access	**Execution**
Successful exploitation of the log4j vulnerability may grant initial access using the following ATT&CK techniques: T1190 (Splunk, Trend Micro)	T1203, T1059 (Splunk, Trend Micro)
Credential Access	**Lateral Movement**
T1003.008 (Trend Micro)	T1021.002 (Trend Micro)
Impact	
T1496, T1498 (Trend Micro)	

[a] TSA Surface Operations mission address entities in the Transportation Sub sector of U.S.: Pipelines, Highway and Motor Carrier, Mass Transit and Passenger Rail, Freight Rail, and certain conveyances within Maritime.

[b] A High Risk is likely to result in a concerning impact and or compromise surface transportation modes.

[c] Malicious cyber actors consist of Nation State (APT), Criminal Groups, Hacktivists, Insider Threats, and Opportunistic hackers.

Mitigation Recommendation:

For asset owners across the surface transportation systems subsector, TSA recommends the following on the part of risk mitigation efforts:

- Review software asset inventory for products affected by Log4j (both cloud and on-premises software).
  - Further guidance can be found on CISA's log4j webpage (CISA).
  - Prioritize assets that:
    - Have external internet exposure
    - Are considered a part of a critical process
- Apply immediate workarounds to mitigate the log4j vulnerability
  - CISA log4j Guidance
- Patch vulnerable systems that can be patched without impact to the safe operation of critical systems.
  - Review vendor patching guidance for critical systems
  - Test patches
  - Implement tested and vendor approved patches immediately
- Review system logs to identify further areas where log4j may be in use
  - Conduct historical analysis dating to at least 1 December, 2021 for any assets running log4j to ensure no follow-on payloads were downloaded
- Ensure log4j related impacts to an IT asset will not impact an OT critical asset.
  - Ensure network segmentation and isolation capabilities are in place that enable the OT system to operate with minimal impact during any related cyber event.
  - Review network access control lists to ensure they are refined to the minimal access necessary for the critical process to function.
- Implement application layer inspection capabilities to prevent/detect and alert to log4j related exploits
- Implement and exercise other host and network based heuristics to detect log4j related events and investigate each event.
- Review and adopt additional guidance, IOCs, and updates from CISA

To adopt these mitigations effectively it is generally recommended that an organization have a tier 2 adoption of the NIST Cybersecurity Framework, or a related framework / standard at a relative adoption level. Minimal areas of CSF impact are detailed below:

Table 2. Minimum CSF Affected Areas

Log4J Affected Cybersecurity Framework Mitigation Areas	
Identify (ID)	ID.RM-3, RD.RM-2, ID.RM-1, ID.RA-6, ID.RA-5, ID.RA-4, ID.RA-3, ID.RA-2, ID.RA-1, ID.GV-4, ID.GV-1, ID.BE-4, ID.BE-3, ID.BE-2, ID.BE-1, ID.AM-5, ID.AM-2, ID.AM-3
Protect (PR)	PR.PT-4, PR.PT-1, PR.IP-12, PR.IP-10, PR.IP-9, PR.IP-8, PR.IP-3, PR.IP-1, PR.AC-7, PR.AC-5
Detect (DE)	DE.DP-4, DE.DP-3, DE.CM-8, DE.CM-6, DE.CM-4, DE.CM-1, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5
Respond (RS)	RS.MI-1, RS.MI-2, RS.MI-1, RS.AN-5, RS.AN-4, RS.AN-3, RS.AN-2, RS.AN-1, RS.CO-5, RS.CO-4, RS.CO-3, RS.CO-2, RS.CO-1, RS.RP-1
Recover (RC)	RC.CO-3, RC.RP-1

Known Affected/Unaffected OT Software Vendors:

This list is not comprehensive. As the situation evolves, CISA will provide other resources to follow and track vulnerable software vendors.[1]

Siemens	https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf
Schneider Electric	https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp
Hitachi	https://www.hitachienergy.com/us/en/offering/solutions/cybersecurity/alerts-and-notifications
GE	https://digitalsupport.ge.com/en_US/Alert/GE-Security-Advisories
WindRiver	https://www.windriver.com/security/vulnerability-responses/apache-log4j
Inductive Automation	https://support.inductiveautomation.com/hc/en-us/articles/4416204541709-Regarding-CVE-2021-44228-Log4j-RCE-0-day
CodeSys	https://www.codesys.com/security/security-reports.html

Additional Resources:

The following link offers additional information:

CISA Apache Log4j Vulnerability Guidance for the latest information. (CISA).

Sources

[1] CISA Log4j Software List, https://github.com/cisagov/log4j-affected-db, accessed 14 December 2021.