APACHE LOG4J VULNERABILITY

5 Steps to Help Manage the Mayhem

At Armis, our mission is to enable enterprises to adopt new connected devices without fear of compromise by cyber attack across IT/OT/IoT/IoMT managed and unmanaged assets, both on the network and in the cloud. To help you navigate your response to the Log4j vulnerability, we've outlined a list of best practices to follow for this or any zero-day vulnerability.

1. ASSET VISIBILITY

Make sure you have a broad understanding of your entire organization's attack surface. The Armis platform sees and identifies every asset for 100% visibility across managed and unmanaged IT/OT/IoT/IoMT assets, both on the network and in the cloud.

2. RISK ASSESSMENT

Find out which devices in your environment are vulnerable or need further assessment to confirm potential exposure. The Armis platform can help you map out the devices in your environment running Apache/Java and other applications. It can identify specific devices requiring further review (e.g., confirming exact software versions) and hone in on specific configurations or deployments potentially impacted by such exposures.

3. THREAT ASSESSMENT

Determine if your organization is experiencing an active exploitation attempt or if a malicious threat actor has already successfully exploited the vulnerability in your environment. Armis researchers have analyzed the vulnerability and developed queries to identify active attempts to exploit the flaw quickly.

4. PROTECT YOUR ENVIRONMENT

Take steps to manage and reduce your risk exposure. Isolate or quarantine vulnerable systems and initiate patching efforts. Activate active asset management and security so you don't have to wait for the problems to happen; you can manage them continuously. The Armis platform integrates effortlessly with your existing security and management tools, provides an extra layer of protection of an extensive knowledge base that can detect and respond to exploits, protecting assets that haven't been or can't be patched.

5. EMPOWER ACTIONS TO MINIMIZE IMPACT ON YOUR BUSINES

Determine which business services, solutions, or critical infrastructure could be impacted if the vulnerability is exploited. The Armis platform's IP connection mapping provides insights into the breadth of the business impact by illustrating which assets are communicating with other assets that may be compromised.

LOG4J CHECKLIST

- ☐ Get an accurate and complete inventory of everything in your environment running Apache Log4j.
  - **IT assets:** Servers, VMs, Personal devices, network switches, network gateways, etc.
  - **IOT devices:** IP cameras, TVs, DVRs, multimedia players, etc.
  - **OT devices:** PLCs, HMI panels, Remote I/Os, etc.
  - Unmanaged devices and legacy systems
- ☐ Perform a risk assessment to identify which devices are most vulnerable, which devices can be patched and which need further assessment to confirm potential exposure.
- ☐ Identify active exploit attempts and find out if malicious threat actors already successfully exploited the vulnerability in your environment.
- ☐ Protect your devices: Isolate or quarantine vulnerable systems and initiate patching efforts.
- ☐ Keep tracking unpatched systems that remain vulnerable.
- ☐ Continuously assess business impact: What business services, solutions or critical infrastructure could be impacted by this threat?

Get your Log4j risk assessment today at armis.com/log4j