TECHNICAL BRIEF

Mission Secure

Defending Against Log4j Attacks

Log4j is a Java-based logging framework used worldwide in applications, services, and websites. In December 2021, Log4j was revealed to have a critical vulnerability that allows remote code execution via a relatively simple exploit. This vulnerability puts hundreds of millions of devices at risk, including consumer products, enterprise IT assets, and operational technology (OT) devices.

The Cybersecurity and Infrastructure Security Agency (CISA) assigned the Log4j vulnerability a severity level of 10 out of 10 and urged vendors and users to take immediate action. The recommended mitigation is to upgrade to the latest version of Log4j (which eliminates the vulnerability) or to disable the lookup functionality that enables the exploit in older versions.

However, Log4j mitigation presents several challenges. Many organizations will struggle to identify all of the devices in their ecosystems that use Java and need to be updated. For OT users, the required software updates themselves may be impractical and represent a significant risk to critical operations.

Mission Secure Can Help

Mission Secure provides 24/7 protection against cyber threats to operational technology and industrial control systems. Mission Secure’s products are not vulnerable to Log4j attacks themselves, because they do not utilize Java or any framework components that utilize Java.

Furthermore, Mission Secure can help organizations defend their OT and ICS assets against attempts to access critical systems using Log4j or other threat vectors.

Summary

→ **Log4j vulnerabilities affect hundreds of millions of systems** around the world, including OT and ICS assets in manufacturing, supply chain, oil and gas, and other critical industries.

→ **Mission Secure products are not susceptible to Log4j attacks** because they do not utilize Java or any framework components that utilize Java.

→ **Mission Secure helps defend OT and ICS assets against Log4j attacks** by continually monitoring for unfamiliar and unauthorized network connections. Depending on the organization’s security needs, Mission Secure can send connection data to a SIEM for analysis, generate alerts, or take automated action to block unauthorized connections.

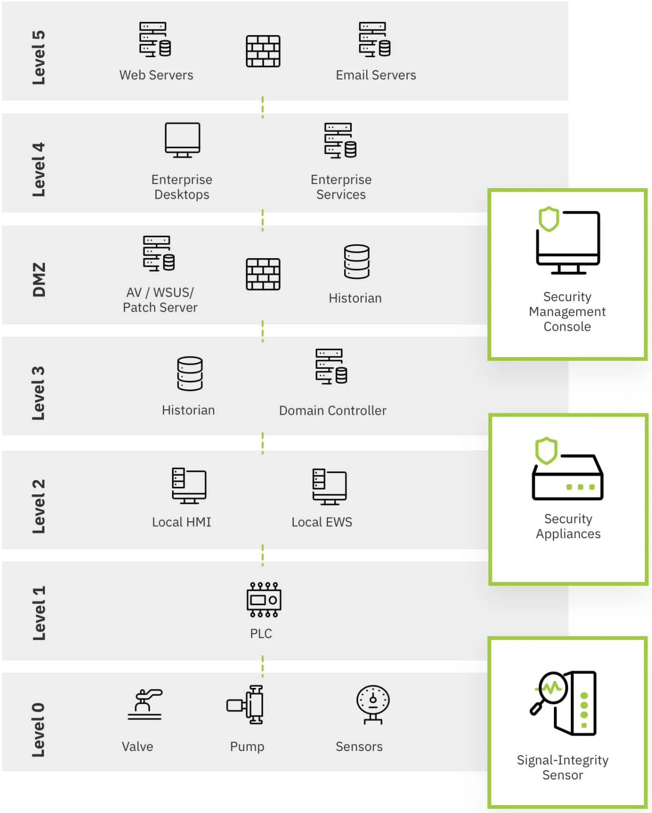
Detecting and Blocking Log4j Attacks with Mission Secure

Mission Secure's integrated cyber protection platform delivers visibility, segmentation, protection, and patented signal integrity monitoring for OT and ICS networks.

The Mission Secure Platform easily deploys in a wide range of operational network environments, providing reliable security at Purdue Model Levels 0, 1, 2, and 3 with a combination of Security Appliances and Signal Integrity Sensors and local management using the Security Management Console.

Organizations can use Mission Secure's **passive monitoring** capabilities to stream network traffic data for SIEM analysis, or to generate alerts on unexpected behavior or unauthorized activity. Organizations can also use Mission Secure's **inline policy enforcement** capabilities to block traffic from unknown sources, effectively preventing a Log4j-based attack.

And with 24/7 managed services as part of Mission Secure's OT-Security-as-a-Service platform, organizations gain the assurance that a team of OT cybersecurity experts are continually on their guard to detect and mitigate cyber threats.



Passive Monitoring

Mission Secure's Security Appliance can be connected to a network tap or SPAN port to identify the devices on an OT network and monitor network traffic for unusual or unauthorized behavior. When unexpected or out-of-policy traffic is detected, Mission Secure's management console can send the data to a SIEM for further analysis, generate an administrative alert, or trigger remediation by the Mission Secure Managed Services team.

Inline Policy Enforcement

When Mission Secure's Security Appliance is implemented inline and configured to block unauthorized traffic, only connections from "known good" whitelisted sources are permitted. Any attempt to gain control of a vulnerable device using Log4j (or other exploit) from an unknown source will be automatically blocked.

Mission Secure

Mission Secure is setting a new standard in OT cyber protection, stopping OT cyber threats head-on. The Mission Secure Platform backed by 24/7 managed services integrates OT visibility, segmentation, protection, threat hunting, and incident response to keep critical operations up and running and safe from harm.

© 2022 Mission Secure and/or its affiliates. All rights reserved.