From: AIG Cyber & Information Security Team

To: product@email.com

Subject: Security Advisory concerning Product Development Staging Environment's Apache Log4j Frameworks

—

Hello Mr. Doe,

AIG Cyber & Information Security Team would like to inform you that a recent Log4Shell vulnerability has been discovered in the security community that may affect product development.

Log4Shell is a zero-day vulnerability found in Log4j, a popular Java logging framework. This vulnerability exists in the action the Java Naming and Directory Interface (JNDI) takes to resolve variables.

Log4Shell is capable of crafting a request to a vulnerable system that causes the system to run arbitrary code execution. This grants the adversary full control over vulnerable networks and systems. They would be able to run any command, as if a server administrator, and exploit any vulnerabilities. This often leads to the deployment of ransomware as well.

We would recommend your team to inventory all assets that make use of the Log4j Java library, and carefully track assets under investigation. The inventory should include all assets, including cloud, regardless of function. For each asset, the following information should be collected: software versions, timestamps of when last updated (and by whom), user accounts on the asset with their privilege level, and the location of asset in your enterprise topology.

Attached are some resources to further aid in identifying assets vulnerable to Log4Shell:

https://github.com/cisagov/log4j-affected-db

https://github.com/CERTCC/CVE-2021-44228_scanner

As far as vulnerability remediation is concerned, we advise your team to treat known and suspected vulnerable assets as compromised. The assets should be isolated until mitigated and verified. Possible isolation methods include: physically removing the asset from the network (i.e., unplug the network cable), moving the asset to a "jail VLAN" with heightened monitoring and security, blocking at the network layer (like a switch or some other device), implementing a firewall (including web application firewall) with strict port control/logging, or restricting the asset's communication, especially to the internet and the rest of the enterprise network.

Another methodology involves patching Log4j and other affected products to the latest version. See the Apache Log4j Security Vulnerabilities webpage, as well as CISA's GitHub for other affected products. Moreover, removing the Jdnilookup.class from the class path from the Log4j JAR files is an effective & commonly used method to mitigate the Log4Shell vulnerability. Again, keeping an inventory of known and suspected vulnerable assets is important throughout the process.

To ensure the mitigation has worked, we advise your organization to scan the patched/mitigated asset with the proper tools and methods listed prior, as well as monitoring the asset closely and remaining alert to changes from vendors for the software on the asset. CISA's GitHub page continually updates the repository as vendors release patches for affected products and patch information. Furthermore, it is advised by the CISA, FBI, NSA, etc. to assume the assets that use Log4j may have been compromised, and to thus initiate hunt procedures accordingly. Conducting vigorous forensic investigations of these assets, along with inspecting monitor accounts across the enterprise that connect to Log4j assets, as well as inspecting changes to configurations made since 12/1/21 and verifying they were intended changes (especially for assets that use Log4j) are all actionary steps we recommend taking to ensure the safety of our critical assets.

Remember to initiate incident response procedures, remain alert to changes from vendors for the software on the asset, and immediately apply updates to assets when notified by a vendor that their product now has a patch for this vulnerability. Continue to monitor Log4j assets closely, and remember to minimize network exposure for all control system devices and/or systems.

Let’s continue working to make sure our organization remains secure and safe for all authorized users and systems.

For any questions or issues, don’t hesitate to reach out to us.

Kind regards,
AIG Cyber & Information Security Team