US Coast Guard Cyber Command
Maritime Cyber Alert 04-21

December 15, 2021

Information Sharing Protocol: TLP-White (https://www.us-cert.gov/tlp)

Actively Exploited Critical Vulnerability in Apache Log4j

Summary:

This Maritime Cyber Alert (MCA) identifies critical vulnerability CVE-2021-44228, rated 10 out of 10 on the Common Vulnerability Scoring System (CVSS) by the National Institute of Standards and Technology. This critical vulnerability affects a ubiquitous logging tool used in the vast majority of Java applications. Numerous types of applications are built using Java including mobile apps, web servers, enterprise applications, embedded systems, and distributed applications. It is estimated more than 100 million devices world-wide across every industry, including the Marine Transportation System (MTS), are impacted. All organizations are urged to take **immediate** action in order to identify and mitigate this vulnerability.

This vulnerability is:

- **Easy to Exploit –** Exploitation is only 12 characters long, and there are a vast number of proof of concepts that are already public.
- **Rapid Automation** – The simplicity of the exploit makes it easy for attackers to automate exploitation.
- **No Network Access or Privilege Restrictions –** Enables the attacker to run remote code execution on a device without any authentication, granting the attacker full control of a system or device.

An unsophisticated remote attacker could exploit this vulnerability to take full control of an affected system.

The following versions are affected: Log4j versions 2.0-beta9 to 2.14.1.

The first known indicator of compromise related to this vulnerability dates back to December 1st, 2021, but it is currently unclear which threat actors are exploiting it. The Cybersecurity and Infrastructure Security Agency (CISA) created a page to be the authoritative source for

information related to this vulnerability. Organizations that identify they are vulnerable are strongly encouraged to regularly check the CISA site for updates on indicators of compromise and mitigation tactics for the foreseeable future.

Mitigations:

There are four recommended steps to mitigate:

1) Scan applications to identify what systems are using vulnerable versions of Log4j. Several free tools are available that can assist with scanning. It is not always readily apparent what systems are using Log4j. Prioritize mitigating public facing applications and critical systems first. However, all vulnerable systems are exploitable and need remediation.
2) Upgrade to Log4j 2.15.0 or later. If you are unable to upgrade, certain versions may allow you to take alternative steps to mitigate the vulnerability.
3) Ensure your security operations center is acting on every alert on systems that are running vulnerable versions of Log4j, even after patching. Review all logs dating back to at least 1 December 2021 to identify potential malicious activity.
4) Update Web Application Firewalls with newest rules. This may prevent attackers using mass scanning and other unsophisticated techniques.

There are still a lot of unknowns related to this vulnerability and organizations are strongly encouraged to continue to check with authoritative sources for new information. Patching may correct this vulnerability, but that alone may not fully protect your organization from compromise.

Resources:

If your organization identifies a vulnerability or has any questions related to this alert, please contact U.S. Coast Guard at: maritimecyber@uscg.mil, or for immediate assistance call the Coast Guard Cyber Command 24x7 Watch at 202-372-2904.