As you're likely aware, Log4Shell, a critical vulnerability in Apache Log4j, is quickly becoming one of the worst software vulnerabilities discovered in many years. We have begun to assist customers by providing remediation guidance and no-cost access to select Tenable products.

Tenable offers a free trial of **Web App Scanning (WAS)** and **Nessus Professional** on our website. If you have a customer that has not taken advantage of a free trial, please contact your Tenable Channel Manager or point your customer to the free trial links above.

Log4Shell allows an unauthenticated, remote attacker to exploit this flaw by sending a specially-crafted request to a server running a vulnerable version of log4j. Because Log4j is one of the most widely used Java libraries by developers today, many applications and systems are impacted by this critical vulnerability.

Using Tenable products, customers and MSSPs will be able to thoroughly assess targets and identify the risk of exploitation from a hacker's perspective. **Web App Scanning (WAS)** compliments the other vulnerability detections in **Tenable.io** to help provide full visibility across the attack surface.

Tenable has enabled the WAS functionality for certain containers that we have determined are at an elevated risk and exposure for Log4Shell. **If you are a Tenable MSSP partner**, some of the **Tenable.io** containers that you manage may have WAS enabled. If you would like to take advantage of **Web App Scanning (WAS)** capabilities for all of your containers, please request a **free trial** or contact your Tenable Channel Manager.

Resources:

- **Share** these new **instructional videos** with your customers to help them learn how to run scans to detect Log4Shell vulnerabilities in their infrastructure using **Tenable.io**, **Tenable.sc**, WAS, and Nessus.
- **Follow** the Tenable **blogs** as they are being continually updated to keep you informed.
    - **CVE-2021-44228: Proof-of-Concept for Critical Apache Log4j Remote Code Execution Vulnerability Available (Log4Shell)**
    - **Apache Log4j Flaw Puts Third-Party Software in the Spotlight**
    - **Apache Log4j Flaw: A Fukushima Moment for the Cybersecurity Industry**
- **Register** for the **Webinar** on December 15, 2:30pm ET, **Vulnerability Alert - Responding to Log4Shell in Apache Log4j**.