Identify Log4j Vulnerability Risk.

Fact sheet

Log4j Assessment

On December 9, 2021, Apache released a security advisory disclosing multiple zero-day exploits identified in a widely used Java logging library called Log4j.

The Log4j vulnerabilities, also known as Log4Shell, allow threat actors to execute unauthorized remote code execution (RCE) and/or unauthorized Denial of Service (DoS) attacks. Log4j is an open-source Java logging library widely used in many applications and services across the globe. The popularity of the Log4j Java logging library significantly increases the attack surface of an organization.

Due to Java's ecosystem, using vulnerability management solutions is a start. A thorough evaluation requires additional steps to identify Log4j vulnerable assets (e.g. nested JAR files) in an environment. Any entity running an application, web site or service that uses the Log4j Java logging library prior to Apache's patch release version 2.17.0 (December 17, 2021) is at risk to these zero-day vulnerabilities.

This Log4j Assessment seeks to:

- Determine if your organization is at risk due to Log4j zero-day exploits.
- Help you make informed decisions about potential mitigation or additional investigatory actions.
- Identify third-party service providers running in the environment that are vulnerable to Log4j exploits.
- Provide independent third-party validation associated with the risk and potential impacts of the Log4j vulnerabilities.

How it works.

Verizon will implement the following methodology:

- Provide remote guidance on collecting in-scope source artifacts, specifically a list of assets running in your organization's environment, VTRAC scanner results for impacted assets, and historical logs associated with impacted assets.
- Receive, on-board, and prepare in-scope source artifacts items and conduct assessment.
- Provide any findings specific to whether Log4j vulnerabilities exist and whether the vulnerabilities were or may have been exploited.
- Advise on any containment, eradication, remediation, or recovery measures.
- Provide a final assessment report with the findings and recommendations.

Learn more.

Verizon's Log4j Assessment enables you to quickly assess whether assets within your organization's environment may be compromised by Log4j vulnerabilities. Verizon provides independent third-party validation of the associated risk and potential impact to your organization along with containment and recommendations for response and mitigation.

For more information, speak to your Verizon Account Manager.

Verizon's Log4j Assessment consists of four phases:

Phase 1 – Identification	Phase 2 – Validation	Phase 3 – Initial investigation	Phase 4 – Risk score reporting
What assets (applications, web sites, or services) are potentially impacted by the Log4j vulnerabilities?	What assets (applications, web sites, or services) are running a vulnerable version of Log4j?	Is there evidence of the vulnerabilities being exploited?	What does the potential risk score mean?

verizon