Log4J Vulnerabilities - Zscaler Resolutions (Updated to 10 Dec 2021)

The information provided below is referred from https://www.zscaler.com/blogs/product-insights/prevent-apache-log4j-java-library-vulnerability-zero-trust-architecture and https://trust.zscaler.com/posts/9581?_gl=1*i2kw4u*_ga*MTU3NDkwMjA2NC4xNjM5OTcyNDE1*_ga_10SPJ4YJL9*MTYzOTk3MjQxNC4xLjEuMTYzOTk3MjkzNC41OQ..&_ga=2.51804011.39101304.1639972415-1574902064.1639972415.

- **CVE Number**

  2021-44228

- **Discovery Date**

  Dec 10, 2021

- **Threat Level**

Critical

- **Response to Log4j**

Recently, a zero-day vulnerability (CVE-2021-44228) was discovered in the popular Apache Log4j logging library, which could allow an attacker full remote code execution. There is evidence that this vulnerability is being exploited in the wild. This logging library is commonly used by enterprise apps and cloud services, with many enterprise deployments supporting private apps. Apache has since released a security update, and provided recommended configurations for earlier versions that mitigates the vulnerability's impact, and we strongly encourage all IT admins to update their software immediately if you haven't already done so.

- **Affected Zscaler Products**

Zscaler has confirmed no impact to its services from the CVE-2021-44228 vulnerability.

- **Zscaler Recommendation**

Security researchers at Alibaba Cloud discovered a zero-day vulnerability, meaning without an emergency security update, every customer running a vulnerable version is at risk. Not only this, but the vulnerability allows full remote code execution, allowing full administrator access to the underlying Apache service and all data within it. In order to exploit this vulnerability, an attacker must first find the app itself. **To stop attackers from doing so**:

1. Minimize your attack surface and make apps invisible
2. Minimize your attack surface and make apps invisible
3. Ensure only authorized users can access apps
4. Prevent lateral movement with user-to-app and app-to-app microsegmentation
   Inspect both inbound and outbound traffic.

If you want to protect your enterprise from zero-day vulnerabilities, retire your firewalls and

VPNs and embrace a true zero trust architecture with the Zscaler Zero Trust Exchange.