calero mdsl

1040 University Ave
Suite 200
Rochester NY 14607
+1 (585) 383 6894
www.caleromdsl.com

Dear Valued Client:

Calero-MDSL is aware of CVE-2021-44228, an actively exploited, high-severity vulnerability in the popular Apache Log4j logging library for Java, which was disclosed publicly via the project's GitHub on December 9, 2021. This vulnerability, which was discovered by Chen Zhaojun of Alibaba Cloud Security Team, impacts Apache Log4j 2 versions 2.0 to 2.14.1.

Upon detection of this emerging threat, Calero-MDSL took immediate action as part of our incident response process and policy, which is in place to ensure that we react appropriately and comprehensively to any actual or suspected security incidents related to information systems and data.

Log4j is one of the most widely deployed Java logging libraries and is widely used in both open- and closed-source software packages. As such, Calero-MDSL Security Response Team are taking a thorough and multi-layered approach to detection and mitigation.

Internal scans of security logs and platforms have been conducted on both internal and external-facing servers, and web application firewalls and intrusion detection & prevention systems have been updated with appropriate patterns to neutralize any ongoing external attacks.

Calero-MDSL's Customer-facing Software Solutions

Results of Calero-MDSL's review to date confirm that our customer-facing platforms **are not vulnerable** because they either take **no dependency on log4j** or **use versions that do not contain the vulnerability**.

Non-customer-facing services

Where non-customer-facing (internal, operational) services have identified log4j dependencies, these servers have been isolated or powered down pending appropriate patching or further mitigation. No customer impact is expected.

As of 12th December 2021, we have found no evidence of exploitation of our servers, nor any residual compromised services.

The Calero-MDSL Security Operations team will continue to scan all services for related vulnerabilities, produce and execute patching or mitigation plans where required, and monitor our SIEM/SOAR tools closely for evidence of attempted or actual exploitation of this vulnerability.

Sincerely,

Simon Mendoza
Chief Technology Officer