SCALA
www.scala.com

Scala Enterprise – Update on CVE-2021-44228 (Apache Log4j 2 Vulnerability)

This communication is to inform you that Scala's R&D team has examined the recent security issue with Log4j 2 Remote Code Execution Vulnerability CVE-2021-44228 (CVSSv3 10.0), and we have assessed that **Scala customers are not affected by this issue**. Details are below.

Log4j 2 Remote Code Execution Vulnerability CVE-2021-44228 (CVSSv3 10.0) is a high severity remote code execution vulnerability in the Apache Log4j2 logging library. This vulnerability allows unauthenticated remote code execution on susceptible systems leveraging the Log4j 2 library, affecting versions 2.0 through 2.14.1. (https://nvd.nist.gov/vuln/detail/CVE-2021-44228)

The Scala Enterprise Product Line does not utilize the Log4j 2 library. Legacy versions of Scala Content Manager (prior to release 11.02) include an implementation of a prior version of the Log4j library (1.2.16) that is unaffected by this exploit.

No further action is required by Scala customers at this time.

Scala continues to monitor the situation as additional information on the exploit surfaces, and will make information available should any additional risks or potential attack vectors surface.

Best regards,

Mark Weidner
VP, Engineering

7 Great Valley Parkway
Suite 300 Malvern
PA 19355

Phone: 610-363-3350
Fax: 610-363-4010