TigerTMS Statement to Vulnerability CVE-2021-44228 v1.0 – 17th December 2021

Summary:

Apache Log4j Remote Code Execution Vulnerability

Document Reference: https://nvd.nist.gov/vuln/detail/CVE-2021-44228

Current Description from NIST as of 16/12/2022

Apache Log4j2 2.0-beta9 through 2.12.1 and 2.13.0 through 2.15.0 JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behaviour has been disabled by default. From version 2.16.0, this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

Impact on TigerTMS Applications, Services, and Infrastructure Summary

TigerTMS do not use Apache Log4j in any applications, services, or infrastructure past or present

List of CERTIFIED UNAFFECTED TigerTMS Applications, Services, and Infrastructure

TigerTMS iLink - All versions

TigerTMS innLine - All versions

TigerTMS iSurf - All versions

TigerTMS iNotify - All versions

TigerTMS Controlled Networks

TigerTMS iCharge - All versions

TigerTMS iGuest - All versions

TigerTMS iPortal - All versions

TigerTMS Cloud Hosting

List of vulnerable TigerTMS Applications, Services, and Infrastructure

N/A

We would like to reassure all users of our software that none of our applications use this technology and therefore there is no risk.

Adrian Seymour

Adrian Seymour

Chief Product Officer