Information Security update

Apache Log4j 2 (CVE-2021-44228)

15 December 2021

Dear Customer

There has been recent press coverage regarding an 'exploit' known as Apache Log4j 2 (CVE-2021-44228). At Tunstall, we take Information Security extremely seriously, and continually scan our environments for known vulnerabilities and security risks.

Over the past few days, we have been made aware of a remote code execution vulnerability that affects multiple versions of the Apache Log4j 2 library. Log4j 2 is an open-source Java logging library developed by the Apache Foundation. It is widely used across many organisations and is present in many services as a dependency. For more information regarding this vulnerability please refer to the following alert from NIST: **https://nvd.nist.gov/vuln/detail/CVE-2021-44228**

We have created a dedicated team to specifically address this latest exploit, and we can confirm that our Telecare (TSP, PNC & DMP) and Telehealth (ICP) services are NOT susceptible to this zero-day exploit. This has been validated using our external security scanning system to ensure this vulnerability is not present in the above services.

Please pass this communication to your Data Protection Officer (DPO) and Head of IT

Should you have any further queries please contact your Account Manager.

Tunstall Healthcare Group Ltd, Whitley Lodge, Whitley Bridge, Yorkshire, DN14 0HR
t: 01977 661234 e: enquiries@tunstall.com w: tunstall.com @TunstallHealth