Update: CVE-2021-44228 (“Apache Log4j”)

Boston Scientific is dedicated to ensuring the safety and security of our products worldwide and has been closely monitoring the remote code execution (RCE) vulnerability impacting Apache Log4j versions 2.14.1 and older. A successful attempt at exploitation would allow an unauthenticated attacker to remotely execute arbitrary code on the vulnerable system. Additionally, security researchers claimed threat actors are actively scanning for vulnerable servers using Apache Log4j and that there have been attempts to exploit this vulnerability in real-world businesses.

CVE-2021-44228 is a high severity RCE flaw which affects the Java-based logging library known as Log4j. The Apache-created library is incorporated into a host of popular frameworks, including Apache Struts2, Apache Solr, Apache Druid, and Apache Flink, which services a variety of popular web-based tools and services.

We have confirmed the following products do not use Apache Log4j and are not affected by the CVE-2021-4228 Log4j vulnerability:

- LABSYSTEM™ Pro EP Recording System
- RHYTHMIA HDx™ Mapping System
- SMARTFREEZE™ Cryoablation system

Our global product cybersecurity team continues to assess if the vulnerability affects any other Boston Scientific products using Apache Log4j. As we complete this analysis, we will provide an update to this bulletin.

For more detail refer to:

- NVD - CVE-2021-44228 (nist.gov)
- CVE - CVE-2021-44228 (mitre.org)

Revision 2 – December 17, 2021