Log4j-Sicherheitslücke

Gültig ab: **20.01.2022**
Betrifft: **burster SW & FW**
Verfasser: OM, MT

Hersteller:
burster
präzisionsmesstechnik gmbh & co kg
Talstraße 1 - 5
D-76593 Gernsbach
Deutschland

Postfach 1432
D-76593 Gernsbach
Deutschland

Tel.: (+49) 07224 645-0
Fax.: (+49) 07224 645-88
E-Mail:info@burster.com
www.burster.de

Inhaltsverzeichnis

Haftungsausschluss

Alle Informationen in der vorliegenden Dokumentation wurden mit größter Sorgfalt erstellt und zusammengestellt und mit wirksamen Kontrollmaßnahmen reproduziert. Diese Dokumentation kann Fehler enthalten und die darin enthaltenen Informationen sowie die entsprechenden technischen Daten können ohne vorherige Ankündigung geändert werden. Ohne vorherige schriftliche Zustimmung des Herstellers ist die Vervielfältigung dieser Dokumentation oder ihre Verarbeitung oder Umgestaltung unter Verwendung elektronischer Systeme, auch auszugsweise, verboten.

Die Informationen in diesem Dokument werden „wie besehen“ ohne jegliche Gewährleistung oder Anspruch auf Richtigkeit bereitgestellt. Bitte haben Sie auch Verständnis dafür, dass wir keine Informationen zu Komponenten von Drittanbietern geben können, die in unserer Software verwendet werden. Sie verwenden die Informationen in diesem Dokument auf eigenes Risiko. burster haftet unter keinen Umständen für direkte oder indirekte Schäden, die durch die Verwendung von Software/Hardware/Links entstehen, auf die in diesem Dokument verwiesen wird.

Allgemeine Informationen

Log4Shell, auch bekannt als CVE-2021-44228 ist eine Sicherheitslücke in Log4j. Log4j ist eine Bibliothek zum Protokollieren von Ereignissen und Fehlern in Java-Anwendungen. Die Implementierungen vor 2013 sind nicht betroffen, da die Schwachstelle „erstmals“ seit 2013 besteht. Vereinfacht ausgedrückt kann ein Hacker einen speziellen String an einen Server senden, der Log4j als Logging-Tool verwendet, und diesen Server zwingen, ein schädliches Java-Objekt von einem Hacker-Server zu laden, um potenziell schädliche Aktionen auf dem betroffenen Server auszuführen. Weitere Informationen finden Sie unter: https://logging.apache.org/log4j/2.x/security.html

Stellungnahme zur Log4j-Sicherheitslücke von burster

Embedded-Geräte:

Burster-Embedded-Geräte basieren im Allgemeinen nicht auf Java-Technologie und verwenden weder Log4j noch Apache Server im Besonderen. Daher sind die burster Embedded-Geräte **nicht betroffen.**

PC Software:

PC Program	Verwendung von Log4j	Betrifft
DigiControl	Keine Verwendung	nicht betroffen
DigiVision	Keine Verwendung	nicht betroffen
2316-P001	Keine Verwendung	nicht betroffen
DigiCal	Keine Verwendung	nicht betroffen
Cable Measurement	Keine Verwendung	nicht betroffen
FMControl	Keine Verwendung	nicht betroffen
9221-P001	Keine Verwendung	nicht betroffen
Burster Instrument Drivers (X86, X64)	Keine Verwendung	nicht betroffen
Serial Console	Keine Verwendung	nicht betroffen
TCP-IP Tool	Keine Verwendung	nicht betroffen
Remote Control Tool	Keine Verwendung	nicht betroffen
UDP Console	Keine Verwendung	nicht betroffen
DigiTEDS	Keine Verwendung	nicht betroffen