Vulnerability of Log4j

		Manufacturer:
© 2022	burster präzisionsmesstechnik gmbh & co kg All rights reserved	burster präzisionsmesstechnik gmbh & co kg

Talstraße 1 - 5
D-76593 Gernsbach
Germany

Postfach 1432
D-76593 Gernsbach
Germany

Valid from: **January 20, 2022**
Applies to: **burster SW & FW**
Reporter: OM, MT

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

Table of Contents

Disclaimer........3

General information........3

Statement of Log4j by burster........3

Disclaimer

All information in the present documentation was prepared and compiled with great care and reproduced in accordance with effective control measures. This documentation may contain errors, and the information it contains and the corresponding technical data are subject to change without notice. Reproduction of any part of this documentation or its processing or revision using electronic systems is prohibited without the manufacturer's prior written approval.

The information in this document is provided on an "as is basis" without any kind of warranty or claim to correctness. Please also have understanding that we cannot provide any information on 3rd party components used in our software. You use the information in this document at your own risk. In no circumstances is burster liable for any direct or indirect damages caused by the use of software/hardware/links referenced in this document.

General information

Log4Shell, also known as CVE-2021-44228 is a security vulnerability in Log4j. Log4j is a library for logging events and errors in Java applications. The implementations before 2013 are not affected because the vulnerability exists "first" since 2013. In simple terms, a hacker can send a special string to a server that uses Log4j as a logging tool and force that server to load a malicious java object from a hacker's server to execute potentially harmful actions on the affected server. You can find more information on: https://logging.apache.org/log4j/2.x/security.html

Statement of Log4j by burster

Embedded devices:

Burster embedded devices are not based on Java technology in general and neither use Log4j nor Apache Server partically. Therefore, the burster embedded devices are **not affected.**

PC Software:

PC Program	Usage of Log4j	Affects
DigiControl	no usage	not affected
DigiVision	no usage	not affected
2316-P001	no usage	not affected
DigiCal	no usage	not affected
Cable Measurement	no usage	not affected
FMControl	no usage	not affected
9221-P001	no usage	not affected
Burster Instrument Drivers (X86, X64)	no usage	not affected
Serial Console	no usage	not affected
TCP-IP Tool	no usage	not affected
Remote Control Tool	no usage	not affected
UDP Console	no usage	not affected
DigiTEDS	no usage	not affected