Technical Bulletin

To: DW® Customers

Date: December 15, 2021

Re: Log4j Software Vulnerability Statement

Log4j Software Vulnerability Statement

Dear Digital Watchdog Partner,

This technical bulletin is being provided to address the growing concerns with the recent "Log4Shell" software vulnerability. We are here to reassure you that Digital Watchdog's products remain unaffected by this news and are not vulnerable to the Log4J zero-day exploit.

This past Friday (12/10/2021) the Apache Software Foundation discovered and disclosed a severe vulnerability that exists in "Log4J", a widely used JAVA-based logging library that was developed by the Apache Software Foundation. It was found that the vulnerability allowed code injection on targeted systems.

- For more information: CVE-2021-44228

Please be assured that the DW Spectrum IPVMS software, DW Blackjack Series, VMAX Series, and the MEGApix IP Camera Series devices do not use the JAVA programming language that the Log4J vulnerability is derived from. Instead, Digital Watchdog systems use JavaScript (.JS format), a completely different scripting language from the JAVA programming language.

Digital Watchdog customers do not need to take any action or alterations with their DW systems or products. It is recommended to keep the firmware and software versions of DW products up-to-date to ensure that current cybersecurity standards and function updates are implemented on your surveillance system(s).

For More Information or Technical Support

DW Technical Support:

Toll-free: 866.446.3595

digital-watchdog.com/contact-tech-support/

866.446.3595 sales@digital-watchdog.com www.digital-watchdog.com

Rev: 12/21