Technical Bulletin

To: DW® Customers

Date: December 13, 2021

Re: Log4J Logging Framework Concerns

Log4J (JAVA) Framework Exploit Concerns

DW Spectrum VMS Suite Cybersecurity

This past Friday (12/10/2021), a severe vulnerability existing in Log4J, a widely used Java-based logging library developed by the Apache Software Foundation, was discovered to enable code injection on affected servers.

This technical bulletin is to inform you that the DW Spectrum VMS suite does not use JAVA and is not vulnerable to the Log4J zero-day exploit.

The DW Spectrum VMS suite consists of:

- DW Spectrum Mediaserver
- DW Spectrum Desktop Client
- DW Spectrum Mobile Client
- DW Spectrum WebAdmin
- DW Spectrum Cloud

Log4J & Log4JS False Positive Detections

There are tools online that can be used to check your system for vulnerabilities, such as the Log4J exploit. However, in the case of DW Spectrum, a false positive may instead appear as a "*log4j***s**" detection, which should not be mistaken by users as a vulnerability.

*Log4**js*** is used by the JavaScript (.js format) scripting language, completely different from the JAVA (.JAVA format) programming language. JavaScript (and *log4js*) is not affected by the Log4J zero-day exploit.

More information on this vulnerability can be found here:

- CVE-2021-44228

Related Articles

- How Secure is DW Spectrum?
- Cyber Security and DW Spectrum

For More Information or DW Technical Support

Toll-free: 866.446.3595

Request Form: https://digital-watchdog.com/contact-tech-support/