1. OVERVIEW

Officially named CVE-2021-44228, (in the Common Vulnerabilities and Exposures database) this security vulnerability is commonly being referred to as "Log4j". Log4j is a logging library made by the Apache Software Foundation and is used extensively in many services and applications. The security risk found with Log4j allows hackers to execute remote commands on a target system.

2. EVERTZ EXPOSURE

Evertz, as a company, is not vulnerable to these exploits.

We continue to investigate on a product-by-product basis, but can conclusively say that most of our product lines are not affected. These unimpacted products include, but are not limited to: MAGNUM, VUE, VLPro and DreamCatcher as well as the majority of our 3484/3482/3480 platforms (TXEs and MUXers), Mulitiviewers, MMA10G and UXP, RF & 78xx series platforms.

The security vulnerability has been found in the Mediator Java library. To prevent a possible remote execution attack, we are recommending all Mediator-X systems have their logging configuration updated. This will resolve all services within Mediator-X that use a log4j2 version >= 2.10. Customers will be contacted by the Mediator project team to arrange deployments of this patch.

InSITE is also vulnerable.Evertz has published service pack 18 to address the issue. Evertz support teams are working to roll out this patch.

Should you have any inquiries or to request information on these mitigations, please contact our Log4j support team at Log4j@evertz.com.