Galaxy Control Systems

RE: CVE-2021-44228: Apache Log4j2 Zero-Day Exploited (Log4Shell)
Date: December 15, 2021

Galaxy Control Systems is aware of the recently disclosed security issue relating to the open-source Apache "Log4j2" utility (CVE-2021-44228).

Galaxy Software and Hardware has **no vulnerability** with our current or past software or hardware releases.

Software: System Galaxy, Launch Point, and Galaxy Mobile Apps

Hardware: 400, 508, 508i, 600, 635 series controllers

What is Log4J?

Log4J is an open-source Java-based logging tool available from Apache. It can perform network lookups using the Java Naming and Directory Interface to obtain services from the Lightweight Directory Access Protocol. Log4j will interpret a log message as a URL, go and fetch it, and even execute any executable payload it contains with the full privileges of the main program. Exploits are triggered inside text using the ${} syntax, allowing them to be included in browser user agents or other commonly logged attributes.

Informational Resources

Update for Apache Log4j2 Security Bulletin (CVE-2021-44228) (amazon.com)

https://nvd.nist.gov/vuln/detail/CVE-2021-44228

https://cisa.gov/uscert/apache-log4j-vulnerability-guidance

Daniel Gramlich
Technical Director
Galaxy Control Systems

GALAXY CONTROL SYSTEMS
3 North Main Street
Walkersville, MD 21793
301.845.6600 Phone
301.898.3331 Fax