Automated Logic

Background:
On December 10, 2021, CVE-2021-44228 was published as a Remote Code Execution vulnerability in the Apache Log4j library, a Java-based logging utility. This vulnerability allows an attacker who can control log messages to execute arbitrary code loaded from attacker-controlled servers. Apache quickly released Log4j 2.15.0 to resolve the vulnerability, the vulnerability is trivial to exploit, and researchers have logged attackers scanning and attempting to compromise vulnerable devices.

PSIRT Statement:
Automated Logic, in collaboration with our Engineering and Global Product Cybersecurity organizations, worked rapidly and thoroughly to investigate any potential impacts of CVE-2921-44228 within our portfolio of offerings. **On December 13, 2021, our Product Security Incident Response Team (PSIRT) was able to conclude that no version of WebCTRL or any of our controller products are impacted by the Remote Code Execution vulnerability in the Apache Log4j library (CVE-2021-44228).**

On December 10, 2021, CVE-2021-44228 was published as a Remote Code Execution vulnerability in the Apache Log4j library, a Java-based logging utility. This vulnerability allows an attacker who can control log messages to execute arbitrary code loaded from attacker-controlled servers. Apache quickly released Log4j 2.15.0 to resolve the vulnerability.

December 13, 2021, CVE-2021-4104 Increases the scope to include Log4j 1.2.x

December 14, 2021, CVE-2021-45046 It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. Apache responded with the release of Log4j 2.16.

December 18, 2021, CVE-2021-45105 It was found that the fix to address CVE-2021-45046 in Apache Log4j 2.16 did not protect from uncontrolled recursion from self-referential lookups. This results in a StackOverflow error that will terminate the process, also known as a DOS (Denial of Service) attack. Apache responded with the release of Log4j 2.17.

Our experts have evaluated the use of Log4j 1.2.x in WebCTRL 7 and determine it is not impacted by CVE-2021-4104, however, out of an abundance of caution and in alignment with our firm commitment to ensuring the security posture of our offerings, ALC will remove Log4j 1.2.x in the next patch of WebCTRL 7.

None of our controllers utilize Log4j in any variant in their firmware so they do not have any related vulnerabilities.

More information about vulnerabilities are provided by the Apache Foundation at Log4j – Apache Log4j Security Vulnerabilities.

General Information:
For more information about the Remote Code Execution vulnerability referenced by CVE-2921-44228, please visit the Apache Foundation at Log4j – Apache Log4j Security Vulnerabilities.

About Global Product Cybersecurity:
At Automated Logic, system and operational security is integral. To ensure outcomes, research and development teams leverage Global Product Cybersecurity – a team of highly experienced and credentialed veterans; diverse and dynamic cybersecurity domain experts who've maintained prominent roles and responsibilities in designing, building, and operating highly secure complex systems.

Our Product Security Incident Response Team (PSIRT) focuses on the identification, assessment, and disposition of the risks associated with security vulnerabilities within all of our products, offerings, solutions, components and/or services. PSIRT is a dedicated team of first responders responsible to deliver advanced support designed to contain and minimize the spread and impact of a product security event, incident, breach, and/or crises.

For more information about Global Product Security and PSIRT, please visit us as:
https://www.corporate.carrier.com/product-security/

Or you may contact us at: productsecurity@carrier.com