Olympus Response to LOG4J Vulnerability (CVE-2021-44228)

Original Release Date: December 22, 2021 | Last Revised Date: December 22, 2021

Note: This communication is the result of initial and ongoing analysis and represents all actions taken by Olympus as of the last revised date. As a result, the content may change as information of the vulnerabilities are released, or additional actions are completed.

Olympus is aware of and currently monitoring ongoing developments related to the recent public reports of various vulnerabilities that affect the Apache Log4j2 versions 2.0-beta9 through 2.12.1 and 2.13.0 through 2.15.0, collectively known as LOG4J. Successful exploitation of this vulnerability can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.

Full information on the vulnerabilities can be found at the following Information Technology Laboratory's National Vulnerability Database link:

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

Olympus Actions & Mitigation Plan

Olympus consistently strives to enhance the security of our products. As such, a global team has been coordinated and has investigated which Olympus products may be affected by these vulnerabilities.

At this time, no medical product developed by Olympus have been found vulnerable to the known LOG4J vulnerability.

This page will be updated as new information becomes available.