# Security Advisory For Apache's Log4j versions 2.0-beta9 to 2.14.1 (CVE-2021-44228)

**Published Date:** December 16, 2021

## SUMMARY

STERIS is aware of the recently announced critical vulnerability affecting Apache's Log4j versions 2.0-beta9 to 2.14.1 (CVE-2021-44228). This component is a java-based, library component that is simple to exploit and provides the attacker full remote code execution. It is already being actively exploited. It is also widely used by both enterprise apps and cloud services for logging purposes. The vulnerability has been classified as critical per CVE-2021-44228. For a more detailed description of this vulnerability, it is recommended that Customers review the information provided by Apache and CISA. Links are provided in the section below labeled as Additional Information for your convenience.

## RESPONSE

Our development teams are actively assessing our products and solutions for potential presence of this vulnerability and associated impact so that we can take the appropriate action. To date, STERIS has assessed the list of STERIS products below. We have determined that these products do not contain the vulnerable component and are, therefore, not impacted by the critical vulnerability reported in CVE-2021-44228.

Additionally, as of the writing of this advisory, there are no known reported incidents involving STERIS products or solutions.

**Cantel IPT Product Lines**

Advantage, Advantage Plus, DSD Edge, EndoDry, RapidAER, Endora, Canexis 1.0, ConnectoHIS, ScopeBuddy+, DSD-201, CER Optima, Renatron

**STERIS IPT Product Lines**

ConnectAssure Technology, SPM® Surgical Asset Tracking Software, CS-iQ® Sterile Processing Workflow Management Software

Washer/Disinfectors

- AMSCO® 2000 SERIES WASHER DISINFECTORS
- AMSCO® 3000 SERIES WASHER DISINFECTORS
- AMSCO® 5000 SERIES WASHER DISINFECTORS
- AMSCO® 7000 SERIES WASHER DISINFECTORS
- RELIANCE® 444 WASHER DISINFECTOR
- RELIANCE® SYNERGY WASHER DISINFECTOR
- RELIANCE® VISION 1300 SERIES CART AND UTENSIL WASHER DISINFECTORS
- RELIANCE® VISION MULTI- CHAMBER WASHER DISINFECTOR
- RELIANCE® VISION SINGLE CHAMBER WASHER DISINFECTOR

Steam Sterilizers:

- AMSCO® 400 MEDIUM STEAM STERILIZER

- AMSCO® 400 SMALL STEAM STERILIZERS
- AMSCO® 600 MEDIUM STEAM STERILIZER
- AMSCO® CENTURY® MEDIUM STEAM STERILIZER
- AMSCO® CENTURY® SMALL STEAM STERILIZER
- AMSCO® EAGLE® 3000 SERIES STAGE 3 STEAM STERILIZERS
- AMSCO® EVOLUTION® FLOOR LOADER STEAM STERILIZER
- AMSCO® EVOLUTION® MEDIUM STEAM STERILIZER

Sterility Assurance Incubators:
- CELERITY™ HP INCUBATOR
- CELERITY™ STEAM INCUBATOR
- VERIFY™ INCUBATOR FOR ASSERT™ SELF-CONTAINED BIOLOGICAL INDICATORS

Liquid Chemical Sterilant Processing System:
- SYSTEM 1® endo LIQUID CHEMICAL STERILANT PROCESSING SYSTEM

Low Temperature Sterilization Systems:
- V-PRO® 1 LOW TEMPERATURE STERILIZATION SYSTEM
- V-PRO® 1 PLUS LOW TEMPERATURE STERILIZATION SYSTEM
- V-PRO® MAX 2 LOW TEMPERATURE STERILIZATION SYSTEM
- V-PRO® MAX LOW TEMPERATURE STERILIZATION SYSTEM
- V-PRO® S2 LOW TEMPERATURE STERILIZATION SYSTEM

**SecureCare Services**
SecureCare® ProConnect® Technical Support Services

**OR Integration Product Lines**
HexaVue™ Integration System, IDSS Integration System, Harmony iQ® Integration Systems, HexaVue™ Connect Software, Harmony iQ Perspectives® Image Management System, Clarity Software

**STERIS PeriOperative® Product Lines**
Situational Awareness for Everyone® Display (S.A.F.E.), RealView® Visual Workflow Management System, and ReadyTracker

Also, our PeriOperative, OR Integration and CS-iQ Products are designed to integrate with hospital applications and may utilize a third-party software component called MIRTH Connect that incorporates an earlier version of Apache Log4j that is not included in the list of Apache Log4j versions impacted in CVE-2021-44228.

**STERIS remains committed to continuously making security enhancements to our systems to protect our Customers and products. We will continue to assess and monitor the situation. Should we determine that any of our products or solutions are impacted, we will update our security advisory accordingly.**

**If you have questions regarding this notice, please contact your local IT Administrator or your STERIS representative.**

**Additional Links**

- Log4j – Apache Log4j Security Vulnerabilities
- Apache Releases Log4j Version 2.15.0 to Address Critical RCE Vulnerability Under Exploitation | CISA
- CVE-2021-4104- Red Hat Customer Portal
- https://github.com/nextgenhealthcare/connect/discussions/4892#discussioncomment-1789526
- https://www.zdnet.com/article/security-warning-new-zero-day-in-the-log4j-java-library-is-already-being-exploited/
- https://nvd.nist.gov/vuln/detail/CVE-2021-44228
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228