OpenBlue
Cyber Solutions

Johnson Controls

Log4Shell

December 22, 2021

JCI-PSA-2021-23 v9
CVE-2021-44228

Johnson Controls endeavors to provide its customers with resilient products throughout the product lifecycle, including the design, sourcing, development, deployment, support, and retirement of products.

Overview:
Johnson controls is aware of reports of a vulnerability known as Log4Shell related to Apache Log4j (a logging tool used in many Java-based applications) disclosed on December 9, 2021. We continue to analyze this remote code execution vulnerability (CVE-2021-44228) and assess Johnson Controls products for potential impact.

As Johnson Controls and the industry at large continue to gain a deeper understanding of the impact of this vulnerability, we will publish technical information to help customers detect, investigate, and mitigate attacks, as well as provide guidance on how to increase resilience against related threats.

The tables below identify products for which we have completed our analysis and indicates the status of each. For products not listed, analysis is still underway. This product security advisory is being continuously updated as more information becomes available.

Johnson Controls On-Premise Products

Product	Version	Status (Impacted/Remediated)	Analysis Date
BIRS	All supported versions	Not Impacted	December 22, 2021
C•CURE Web	All supported versions	Not Impacted	December 21, 2021
C•CURE Server	All supported versions	Not Impacted	December 21, 2021
C•CURE Client	All supported versions	Not Impacted	December 21, 2021
Connected Equipment Gateway (CEG)	All supported versions	Not Impacted	December 21, 2021
P2000	All supported versions	Not Impacted	December 21, 2021
S321-IP (P2000)	All supported versions	Not Impacted	December 21, 2021
CK721-A (P2000)	All supported versions	Not Impacted	December 21, 2021
C•CURE-9000	2.60 (All versions)	Not impacted	December 20, 2021
C•CURE-9000	2.70 (All versions)	Not Impacted	December 20, 2021
iSTAR	All supported versions	Not Impacted	December 20, 2021
BCPro	All supported versions	Not Impacted	December 20, 2021
exacqVision WebService	All supported versions	Not Impacted	December 20, 2021
exacqVision Client	All supported versions	Not Impacted	December 20, 2021
exacqVision Server	All supported versions	Not Impacted	December 20, 2021
VideoEdge	5.x	Not Impacted	December 20, 2021
Sur-Gard Receivers	All supported versions	Not Impacted	December 17, 2021
PowerSeries Pro	All supported versions	Not impacted	December 17, 2021
PowerSeries NEO	All supported versions	Not Impacted	December 17, 2021
Qolsys IQ Panels	All supported versions	Not Impacted	December 17, 2021
Kantech EntraPass	All supported versions	Not Impacted	December 17, 2021

DLS	All supported versions	Not Impacted	December 17, 2021
Tyco AI	All supported versions	Not Impacted	December 17, 2021
Illustra Insight	All supported versions	Not Impacted	December 17, 2021
Illustra Cameras	All supported versions	Not Impacted	December 17, 2021
CEM Hardware Products	All supported versions	Not Impacted	December 17, 2021
CEM AC2000	All supported versions	Not impacted	December 17, 2021
Facility Explorer	14.x	Not Impacted	December 16, 2021
Metasys Products and Tools	All supported versions	Not Impacted	December 16, 2021
victor/ C•CURE-9000 Unified	3.91.x / victor 5.6.1 / C•CURE-9000 2.90	Not Impacted	December 16, 2021
victor/ C•CURE-9000 Unified	3.81.x / victor 5.4.1 / C•CURE-9000 2.80	Not Impacted	December 16, 2021
victor	5.x	Not Impacted	December 16, 2021
C•CURE-9000	2.80.x (all 2.80 versions)	Not impacted	December 16, 2021
C•CURE-9000	2.90.x (all 2.90 versions)	Not Impacted	December 16, 2021

Johnson Controls OpenBlue

Product	Status (Impacted/Remediated)	Date
OpenBlue Bridge	Remediated	Remediation date 12/21/2021
OpenBlue Twin	Not Impacted	Analysis date 12/21/2021
OpenBlue Enterprise Manager	Not Impacted	Analysis date 12/18/2021
OpenBlue Cloud	Not Impacted	Analysis date 12/17/2021
OpenBlue Active Responder	Not Impacted	Analysis date 12/17/2021
OpenBlue Risk Insight	Not Impacted	Analysis date 12/17/2021
OpenBlue Workplace	Not Impacted	Analysis date 12/16/2021
OpenBlue Chiller Utility Plant Optimizer	Not Impacted	Analysis date 12/16/2021
OpenBlue Connected Chiller	Not impacted	Analysis date 12/16/2021
OpenBlue Location Manager	Not Impacted	Analysis date 12/15/2021

Johnson Controls Cloud Products

Product	Status (Impacted/Remediated)	Date
Connect24	Not Impacted	Analysis date 12/21/2021
DataSource	Not Impacted	Analysis date 12/21/2021
Xaap	Not Impacted	Analysis date 12/21/2021
RFID Overhead360° Backend	Remediated	Remediation date 12/21/2021
Shoppertrak Shopper Journey	Not Impacted	Analysis date 12/21/2021
Shoppertrak Perimeter Apps	Not Impacted	Analysis date 12/21/2021
Shoppertrak Video Analytics	Not Impacted	Analysis date 12/21/2021
Shoppertrak Market Intelligence	Not Impacted	Analysis date 12/21/2021
Shoppertrak Analytics (STaN) - Traffic	Not Impacted	Analysis date 12/21/2021
TrueVue Cloud	Not Impacted	Analysis date 12/21/2021
CloudVue Web	Not Impacted	Analysis date 12/17/2021
CloudVue Gateway	Not Impacted	Analysis date 12/17/2021
Athena	Not Impacted	Analysis date 12/16/2021

*Note that solutions may involve additional components still under evaluation.

Johnson Controls will continue to monitor this dynamic situation and will publish mitigation recommendations, patches or product updates at our product security advisory site located here: https://www.johnsoncontrols.com/cyber-solutions/security-advisories.

Secure Product Deployment Guidance:
We recommend reviewing product hardening and deployment guides to ensure that products have been deployed in accordance with product design and operations requirements.

- Most Johnson Controls on-premise products: https://www.johnsoncontrols.com/cyber-solutions/security-advisories

- Metasys: https://docs.johnsoncontrols.com/bas/r/Metasys/en-US/Network-and-IT-Guidance-Technical-Bulletin/11.0?filters=docnumber~%2522LIT-12011279%2522

Government Guidance:
https://www.cisa.gov/uscert/ncas/current-activity/2021/12/10/apache-releases-log4j-version-2150-address-critical-rce

Disclosure Practices
Johnson Controls practices coordinated disclosure and has been recognized by MITRE as a Common Vulnerability and Exposures (CVE) Numbering Authority (CNA). Accordingly, Johnson Controls is permitted to self-report to the publicly accessible United States National Vulnerabilities Database. This capability is incorporated into our Product Security Incident Response (PSIR) and vulnerability management process. Product Security Advisories are posted on the Cyber Solutions section of our website at https://www.johnsoncontrols.com/cyber-solutions/security-advisories.

For more information, please visit http://www.johnsoncontrols.com/ or to learn about Johnson Controls holistic approach to cybersecurity visit https://www.johnsoncontrols.com/cyber-solutions.

Sincerely,

Cyber Solutions Team