OpenBlue
Cyber Solutions

Johnson Controls

Apache Log4j

December 16, 2021

JCI-PSA-2021-23 v2
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 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.

Our analysis currently indicates that the following products are not affected by the Apache Log4j vulnerability. We continue to assess impact to other supported products and solutions within the Johnson Controls portfolio.

Product	Version	Analysis Date
C•CURE-9000	2.90.x (all 2.90 versions)	December 16, 2021
C•CURE-9000	2.80.x (all 2.80 versions)	December 16, 2021
victor	5.x	December 16, 2021
victor/ C•CURE-9000 Unified	3.81.x / victor 5.4.1 / C•CURE-9000 2.80	December 16, 2021
victor/ C•CURE-9000 Unified	3.91.x / victor 5.6.1 / C•CURE-9000 2.90	December 16, 2021
Metasys Products and Tools	All versions	December 16, 2021
Facility Explorer	14.x	December 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