OpenBlue
Cyber Solutions

Johnson Controls

Spring4Shell

May 20, 2022

JCI-PSA-2022-14 v2
CVE-2022-22965

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 Spring4Shell which is related to vulnerabilities discovered in a widely used Java open-source framework. This issue has been assigned the following identifier: CVE-2022-22965.

We are evaluating products for any potential impact. If a product is identified, Product Security Advisories will be created. Advisories are always published here: https://www.johnsoncontrols.com/cyber-solutions/security-advisories

Product	Version	Status (Impacted/Remediated)	Analysis Date
Illustra Cameras	All supported versions	Not Impacted	May 19, 2022
Visonic PowerManage	All supported versions	Not Impacted	April 15, 2022
Qolsys IQ Cloud	All supported versions	Not Impacted	April 15, 2022
Metasys Products and Tools	All supported versions	Not Impacted	April 15, 2022
C•CURE Web	All supported versions	Not Impacted	April 15, 2022
C•CURE Server	All supported versions	Not Impacted	April 15, 2022
C•CURE Client	All supported versions	Not Impacted	April 15, 2022
C•CURE-9000	All supported versions	Not impacted	April 15, 2022
exacqVision Web Service	All supported versions	Not impacted	April 15, 2022
exacqVision Client	All supported versions	Not impacted	April 15, 2022
exacqVision Server	All supported versions	Not impacted	April 15, 2022
victor	All supported versions	Not impacted	April 15, 2022
P2000	All supported versions	Not impacted	April 15, 2022
S321-IP Network Controller P2000	All supported versions	Not impacted	April 15, 2022
CK721-A Network Controller P2000	All supported versions	Not impacted	April 15, 2022
Sur-Gard Receivers	All supported versions	Not impacted	April 15, 2022
PowerSeries Pro	All supported versions	Not impacted	April 15, 2022
PowerSeries Neo	All supported versions	Not impacted	April 15, 2022
Qolsys IQ Panels	All supported versions	Not impacted	April 15, 2022
Kantech EntraPass	All supported versions	Not impacted	April 15, 2022
OpenBlue Cloud	All supported versions	Not impacted	April 15, 2022

Johnson Controls will continue to monitor this situation and will publish mitigation recommendations, patches or product updates at our product security advisory site located here: Johnson Controls Product 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/ics/Recommended-Practices

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