Product Security Advisory

July 18, 2024

JCI-PSA-2024-04 v2
CVE-2024-0912
ICSA-24-135-03

Overview

Johnson Controls has confirmed a vulnerability impacting Software House C•CURE 9000 v3.00.2.

Impact

Under certain circumstances the Microsoft® Internet Information Server (IIS) used to host the C•CURE 9000 Web Server will log Microsoft Windows credential details within logs.

Affected Versions

- Software House C●CURE 9000 v3.00.2

Mitigation

- Upgrade C•CURE 9000 to version 3.00.2 CU02 or 3.00.3
- Change the password for the impacted windows accounts
- Delete the api.log log file (or remove instances of passwords from the log file with a text editor) located at "C:\Program Files (x86)\Tyco\victorWebServices\victorWebsite\Logs"

Initial Publication Date

May 14, 2024

Last Published Date

July 18, 2024

Resources

Cyber Solutions Website - https://www.johnsoncontrols.com/cyber-solutions/security-advisories
CVE-2024-0912 - NIST National Vulnerability Database (NVD) and CVE®
ICSA-24-135-03 - CISA ICS-CERT Advisories

In addition to the guidance provided in this advisory, the recommendation provided within Johnson Controls Hardening Guide should always be applied to minimize security risk.

Visit the Johnson Controls Trust Center Cybersecurity website to access the latest Hardening Guidelines and best practice in cybersecurity - https://www.johnsoncontrols.com/trust-center/cybersecurity/resources.