Product Security Advisory

August 12, 2021

JCI-PSA-2021-10 v2
CVE-2021-27660
ICSA-21-182-02

Overview

A security vulnerability has been announced affecting all versions of Software House C•CURE 9000 prior to version 2.80. The vulnerability affects the client auto update feature.

Please Note: This is an addendum to the prior release for Software House C•CURE 9000 that was made available on 7/01. This advisory provides additional mitigation guidance.

Impact

An insecure client auto update feature in Software House C•CURE 9000 can allow remote execution of lower privileged Windows programs.

Affected Versions

This affects all versions of Software House C•CURE 9000 prior to 2.80.

Mitigation

Upgrade to version 2.80 or above. If the C•CURE 9000 Auto Update feature in not being used, it is advised that it be uninstalled.

IMPORTANT: Versions prior to 2.60 should first be upgraded to 2.60 Service Pack 2 CU07 or later.

Version 2.60

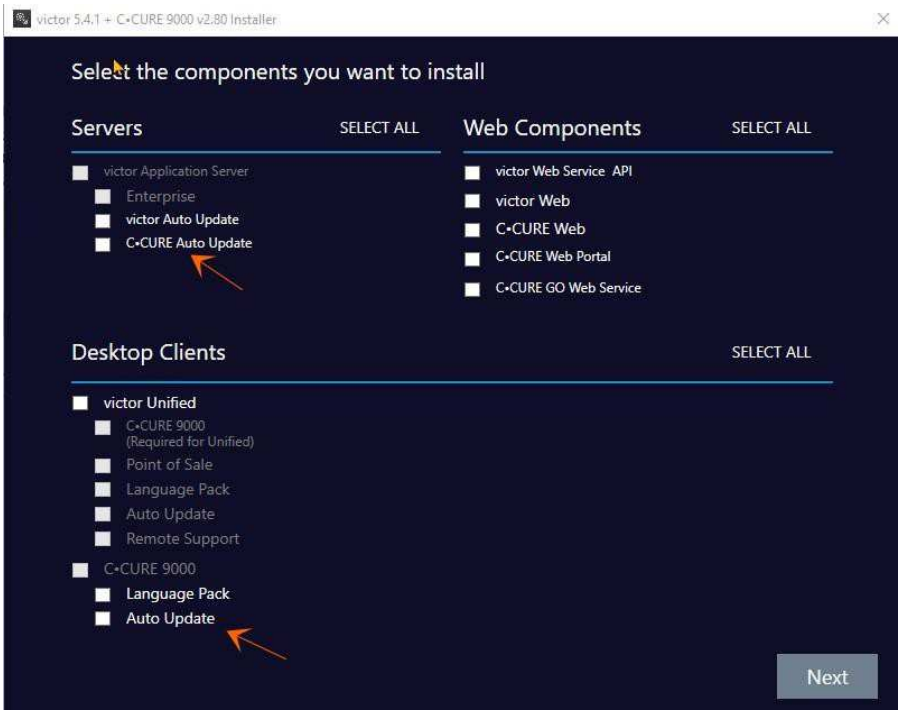
- Apply 2.60 Service Pack 2 CU07 or later.
- On the machine that has the C•CURE 9000 server installed, the service pack will automatically remove the auto update client.
- On remote client machines, when running the service pack, if the Auto Update service is installed, a prompt will ask you if you want to remove the service.
- If you run the service pack in silent mode, you should run it with the optional parameter " /REMOVEAUTOUPDATE" to remove the auto update client.

Version 2.70

- Apply 2.70 Service Pack 2 CU01 or later.
- On the machine that has the C•CURE 9000 server, the service pack will automatically remove the auto update client.
- On remote client machines, when running the service pack, if the Auto Update service is installed, a prompt will ask you if you want to remove the service.
- If you run the service pack in silent mode, you should run it with the optional parameter " /REMOVEAUTOUPDATE" to remove the auto update client.

Version 2.80 & 2.90

- Starting in C•CURE 9000 version 2.80, the client Auto Update feature is a separate install.



- From Windows **Programs and Features**, on the application server, select **C•CURE 9000 Automated Update**, right-click, then select **Uninstall**.
- From Windows **Programs and Features**, wherever the C•CURE 9000 clients (Monitoring Station, Administration Workstation) are installed (and the Auto Update service), select **CCURE9000ClientAutoupdate**, right-click, then select Uninstall.

Technical Support Contact Information

North America & Latin America	Toll Free: 800-507-6268, Option 3 or International: 561-912-6259, Option 3 Hours: 8 AM – 8 PM Eastern Access Technical Support: Access-support@jci.com
EMEA	Toll Free: 800-2255 8926 Direct: +31 475 352 722 Hours: 8 am to 6 pm CET Access Technical Support: Access-support@jci.com

	All license Inquiries: sp-licensing-support@jci.com
ASIA/PACIFIC	Toll free: +800-2255 8926 Direct: +91-80-4199-0994 Hours: 9am to 6pm CST (China Time) and 9am to 7pm IST (India Time) Access Technical Support: Access-support@jci.com All license Inquiries: sp-licensing-support@jci.com
Support Contact List	Complete Support Contact List

Initial Publication Date
July 1, 2021

Last Published Date
August 12, 2021

Resources
Cyber Solutions Website – https://www.johnsoncontrols.com/cyber-solutions/security-advisories
CVE-2021-27660 – NIST National Vulnerability Database (NVD) and MITRE CVE® List
ICSA-21-182-02 – CISA ICS-CERT Advisories