High-Severity Vulnerabilities Found in WellinTech Industrial Data Historian

Cisco's Talos threat intelligence and research unit this week disclosed the details of two high-severity vulnerabilities discovered last year in WellinTech's KingHistorian industrial data historian software.

China-based industrial automation software company WellinTech designed KingHistorian for collecting and processing a 'massive amount' of industrial control system (ICS) data.

Talos researchers discovered that the historian is impacted by two flaws. One of them, tracked as CVE-2022-45124, can allow an attacker who can intercept an authentication packet to obtain the username and password of the legitimate user who logged in to the system.

[Read: Counting ICS Vulnerabilities: Examining Variations in Numbers Reported by Security Firms **]**

The second issue, CVE-2022-43663, can be exploited by sending a specially crafted network packet that triggers a buffer overflow. It's unclear if the flaw can be exploited for arbitrary code execution or only to crash the process.

The vendor was informed about the security holes in December 2022 and released patches earlier this month.

Cisco has not shared any information on the real world impact resulting from the potential exploitation of these vulnerabilities, but based on previous reports from cybersecurity companies, compromising a historian could be

very useful to threat actors.

In January, industrial security firm Claroty disclosed several vulnerabilities found by its researchers in the GE Digital Proficy Historian product. The company warned at the time that the flaws could be exploited for espionage or to cause damage and disruption in industrial environments.

Historian servers can provide access to both IT and OT systems, allowing hackers to leverage compromised devices to gain access to valuable information or move to other systems on the network.

Related: Vulnerability in ABB Plant Historian Disclosed 5 Years After Discovery

Related: Siemens Drives Rise in ICS Vulnerabilities Discovered in 2022

Related: ICS Vulnerabilities Chained for Deep Lateral Movement and Physical Damage

https://www.securityweek.com/high-severity-vulnerabilities-found-in-wellintech-industrial-data-historian/