LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF INFORMATION SECURITY

HC3: Alert

March 08, 2022 TLP: White Report: 202203081700

PTC Axeda agent and Axeda Desktop Server Vulnerabilities

Executive Summary

CISA is aware of a public report, known as “Access:7” that details vulnerabilities found in PTC Axeda agent and Axeda Desktop Server. The Axeda agent and Axeda Desktop Server are web-based technologies that allow one or more people to securely view and operate the same remote desktop, through the Internet. These vulnerabilities can affect medical, Internet of Things (IoT), and embedded devices dependent on the affected product. Successful exploitation of these vulnerabilities could result in full system access, remote code execution, read/change configuration, file system read access, log information access, and a denial-of-service condition.

Report

ICS Advisory (ICSA-22-067-01) PTC Axeda agent and Axeda Desktop Server
PTC Axeda agent and Axeda Desktop Server | CISA

Impact to HPH Sector

The agent and desktop server are used in numerous medical devices across several medical device manufacturers. The following versions of Axeda agent and Axeda Desktop Server, a remote asset connectivity software used as part of a cloud based IoT platform, are affected:

- Axeda agent: All versions
- Axeda Desktop Server for Windows: All versions

Mitigations to these vulnerabilities are included in the above referenced report.

References

Cybersecurity Alert: Vulnerabilities identified in medical device software components: PTC Axeda agent and Axeda Desktop Server
Cybersecurity | FDA

Access:7 vulnerabilities impact medical and IoT devices
Access:7 vulnerabilities impact medical and IoT devices (bleepingcomputer.com)

Contact Information

If you have any additional questions, please contact us at HC3@hhs.gov.

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback