Vantive Product Security Bulletin

RE: Axeda agent and Axeda Desktop Server

Publication Date: March 22, 2022

ISSUE SUMMARY

Vantive is currently monitoring the recently published announcement of vulnerabilities affecting PTC's Axeda agent and Axeda Desktop Server for Windows. These vulnerabilities, also known publicly as "Access:7", were discovered by research firm CyberMDX.

For a more detailed description of these vulnerabilities, it is recommended customers view the information provided by PTC and CISA.

Products in Scope

The products listed below were identified as utilizing the Axeda agents listed in the PTC Advisory:

- Amia (All fielded versions)
- Kaguya (All fielded versions)

RESPONSE

Please note that the Axeda vulnerabilities are not Vantive-specific vulnerabilities. In compliance with Vantive's product security risk governance, potential risk impacts from these reported vulnerabilities were evaluated across Vantive line of products and services.

The fielded Amia/Kaguya devices have additional design features such as integrated firewall and network access control lists for restricting network traffic while communicating securely via TLS with the Axeda Gateway Server. These added security design features protect the devices and mitigate the risk of the reported vulnerabilities. To further strengthen protection, Vantive is working with PTC to upgrade the Amia/Kaguya Axeda agent to the recommended version during 2022.

In the meantime, Vantive will continue to monitor all available information and if Vantive learns any new information related to these vulnerabilities, this bulletin will be updated.

For questions regarding cybersecurity of any Vantive product contact:
global.corp.product.security@vantive.com