The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
03/09/2022

SUBJECT:
Multiple Vulnerabilities in PTC Axeda Agent and Axeda Desktop Server Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in PTC Axeda Agent and Axeda Desktop Server, the most severe of which could allow for remote code execution. PTC Axeda is a cloud based remote access solution commonly used for devices within the healthcare industry. 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.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Axeda agent: All version
- Axeda Desktop Server for Windows: All versions

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in PTC Axeda agent and Axeda Desktop Server, the most severe of which could allow for remote code execution. Details of these vulnerabilities are as follows:

- The affected product uses hard-coded credentials for its UltraVNC installation which could allow for a unauthenticated remote attacker take control of the host operating system. (CVE-2022-25246)
- The affected product may allow an attacker to send certain commands to a specific port without authentication which could allow a remote unauthenticated attacker to obtain full file-system access and remote code execution. (CVE-2022-25247)
- When connecting to a certain port the affected product supplies the event log of the specific service. (CVE-2022-25248)
- The affected product (disregarding Axeda agent v6.9.2 and v6.9.3) is vulnerable to directory traversal which could allow a remote unauthenticated attacker to obtain file system read access via web server. (CVE-2022-25249)
- The affected product may allow an attacker to send a certain command to a specific port without authentication which could allow a remote unauthenticated attacker to shut down a specific service. (CVE-2022-25250)
- The affected product may allow an attacker to send certain XML messages to a specific port without proper authentication which could allow a remote unauthenticated attacker to read and modify the product's configuration. (CVE-2022-25251)
- Improper handling of exceptions could allow a remote unauthenticated attacker to crash the product. (CVE-2022-25252)

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.

RECOMMENDATIONS:

- Upgrade to Axeda agent Version 6.9.2 build 1049 or 6.9.3 build 1051 when running older versions of the Axeda agent.
- Upgrade the Axeda Desktop Server (ADS) to Version 6.9 build 215
- Check manufacturer websites for your affected products for updates, as this will completely mitigate the issue. Companies such as Bayer, Accuray, Eleka, General Electric, and Varian are affected.
    - List of affected devices using Axeda agent: https://learn.cisecurity.org/e/799323/access7-affected-devices-/rrnfl/270573131?h=gcQBqqNE4KMFCAiSaTYzVTIh5hTGnva2U6-nwousOJs
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Apply the Principle of Least Privilege to all systems and services

REFERENCES:

CISA:

https://www.cisa.gov/uscert/ics/advisories/icsa-22-067-01

Bleeping Computer:

https://www.bleepingcomputer.com/news/security/access-7-vulnerabilities-impact-medical-and-iot-devices/

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25246
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25247
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25248
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25249
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25250
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25251
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25252