SCIENCES AND CONSULTING

JOHN WARD CYBERSECURITY BLOGS

YOUR ONLINE RESOURCE FOR TIMELY ANALYSIS, COMMENTARY AND RESOURCES TO KEEP YOU INFORMED ON THE RAPIDLY EVOLVING AND CRITICAL FIELD OF CYBERSECURITY

John Ward – Cyberblog July 2022

ACCESS 7 CYBERSECURITY VULNERABILITY

ACCESS 7 VULNERABILITY

On March 8th of 2022, a report was released by cybersecurity research firm Forescout's Vedere Labs stating that they had discovered seven security vulnerabilities in the Parametric Technology Corporation (PTC)'s Axeda agent. Axeda is an IoT remote access tool that is embedded in devices by an OEM, or original manufacturer, approach. OEM means that the Axeda agent is installed on the device by IoT manufacturers prior to sale to a customer. While the vulnerabilities affect devices in a number of disparate industries such as finance in the case of ATMs and commerce in the case of barcode scanning systems, the Axeda agent is particularly popular in the healthcare industry and utilized in a number of medical devices.

According to Forescout's Vedere Labs the vulnerabilities, collectively dubbed "Access:7", rank in severity scores of between 5.3 and 9.8 on the CVSSv3.1 scale. Three of the vulnerabilities have scores over the threshold for a "critical" vulnerability, which is between 9 and 10. According to a cybersecurity alert issued by the FDA on the same date as Forescout's report on the Access:7 vulnerabilities, successful exploitation of these vulnerabilities could "allow an unauthorized attacker to take full control of the host operating system, resulting in full system access, remote code execution, read/change configuration, file system read access, log information access, and a denial-of-service condition". In conjunction with the Forescout report and the FDA cybersecurity alert, CISA released an ICS-CERT advisory (ICSA-22-067-01), currently in its third iteration, that provides insight into the nature of the vulnerabilities. At the time of public disclosure through Forescout, the FDA and CISA, PTC had developed and made available patches for the vulnerabilities, as well as releasing a public advisory of their own.

In their report Forescout indicated that through an examination of anonymized customer data they were able to determine that 54% of affected devices belonged to the healthcare industry, with the majority being medical imaging and laboratory devices. Forescout was also able to compile a list of more than 100 vendors and 150 devices that used the Axeda solution. The Access:7 vulnerability known as CVE-2022-25256, which scored the highest CVSS score of 9.8, was particularly alarming to industry experts. CVE-2022-25256 allows for access to the AxedaDesktopServer.exe through the exploitation of hard-coded credentials. Hard-coded credentials are a vulnerability in which authentication data, such as user IDs and passwords, are embedded within the source code and thus theoretically accessible to malicious actors. According to Chris Gates, the director of product security at the medical device engineering firm Valentium, the presence of hard-coded credentials in this instance shows "a distinct disregard for creating a secure product".

SCIENCES AND CONSULTING

JOHN WARD CYBERSECURITY BLOGS

YOUR ONLINE RESOURCE FOR TIMELY ANALYSIS, COMMENTARY AND RESOURCES TO KEEP YOU INFORMED ON THE RAPIDLY EVOLVING AND CRITICAL FIELD OF CYBERSECURITY

John Ward – Cyberblog July 2022

ACCESS 7 CYBERSECURITY VULNERABILITY

The Access:7 vulnerabilities present a significant attack surface for malicious actors, and it is important to examine the detection, disclosure, and particularly the coordination processes utilized by the relevant stakeholders to mitigate the impact and risk of the Access:7 vulnerabilities. As the timeline below will indicate the key to mitigating and patching the Access:7 vulnerabilities was the fluid collaboration of independent security researchers, the manufacturing company, and the regulatory/governmental/ISAC entities for the healthcare/medical device space. In their non-binding Postmarket Management of Cybersecurity in Medical Devices guidance from 2016 the FDA indicates that the adoption of a coordinated vulnerability disclosure (CVD) program is a critical component of postmarket surveillance for medical device cybersecurity; an examination of the Access:7 vulnerabilities' discovery, disclosure and remediation will highlight the criticality of a CVD program in the medical device cybersecurity space.

- August 10th, 2021: Security researchers at Forescout's Vedere Labs and Cyber MDX discover the Access:7 vulnerabilities and reported them to PTC through PTC's coordinated vulnerability disclosure process.

  Following this disclosure, PTC requested that Forescout and CyberMDX provide proof-of-concept exploits to show that the Access:7 vulnerabilities could be realistically exploited.

- November 2021: PTC provided coordinated disclosure of the Access:7 vulnerabilities to CISA.

- January 2022: PTC began to notify active vendors believed to be affected by the Access: 7 vulnerabilities.

  During this time Forescout compiled a list of devices that were either currently using, or had previously used, Axeda, and alerted the respective vendors of the vulnerabilities.

  H-ISAC held a session to "help vendors with technical questions and further communication was established afterwards".

John Ward – Cyberblog July 2022

ACCESS 7 CYBERSECURITY VULNERABILITY

- February 2022: The FDA is consulted about the vulnerabilities.

- March 8th, 2022: Forescout, CISA, the FDA and PTC all issue public notifications of the vulnerabilities as well as PTC's mitigation recommendations and patches (these had been provided to previously identified customers and vendors earlier in the disclosure process).

- **Please note: H-ISAC was notified of the vulnerabilities at an undisclosed but pre-public disclosure point in the process at the request of Forescout/CyberMDX and with the consent of PTC and CISA.**

Forescout's own March 8th public disclosure/report on the Access:7 vulnerabilities indicates that the 210 days that passed between Forescout/CyberMDX's vulnerability disclosure to PTC and public disclosure were more than twice the 90-day industry-accepted limit. It is important to note that the complexity and severity of these particular vulnerabilities, as well as the necessary coordination between private and governmental entities necessitated the seemingly slow transition from coordinated to public disclosure. The response to the Access:7 vulnerabilities should be looked at as a significant success for medical device cybersecurity and a roadmap for all relevant stakeholders in the medical device cybersecurity space. The collaboration between private and governmental enterprises and leveraging of the resources available to each enterprise in a thoughtful progression towards public disclosure is indicative of an optimal postmarket risk management and mitigation strategy. As of the writing of this report there have been no reported exploitations of any of the Access:7 vulnerabilities in any medical devices.

Please Note: CyberMDX was responsible for much of the early research and was acquired by Forescout Technologies on February 1st, 2022. This report uses "Forescout" to represent both Forescout Technologies and CyberMDX without distinction.

John Ward – Cyberblog July 2022

ACCESS 7 CYBERSECURITY VULNERABILITY

Resources

- Forescout's Vedere Labs Access:7 Research Report
- Forescout Public Disclosure Blog Post
- PTC-Security Vulnerabilities Identified in the Axeda agent and Axeda Desktop Server
- PTC-Axeda Public Advisory
- CISA-ICS Advisory ICSA-22-067-01 Update C
- FDA-Cybersecurity Alert: Vulnerabilities Identified in Medical Device Software Components: PTC Axeda Agent and Axeda Desktop Server
- Bleeping Computer-Access:7 Vulnerabilities Impact Medical and IoT Devices
- Wired-Critical Bugs Expose Hundreds of Thousands of Medical Devices and ATMs
- MedTechDive-FDA Warns of Cyber Vulnerabilities in Medical Device Software Components

