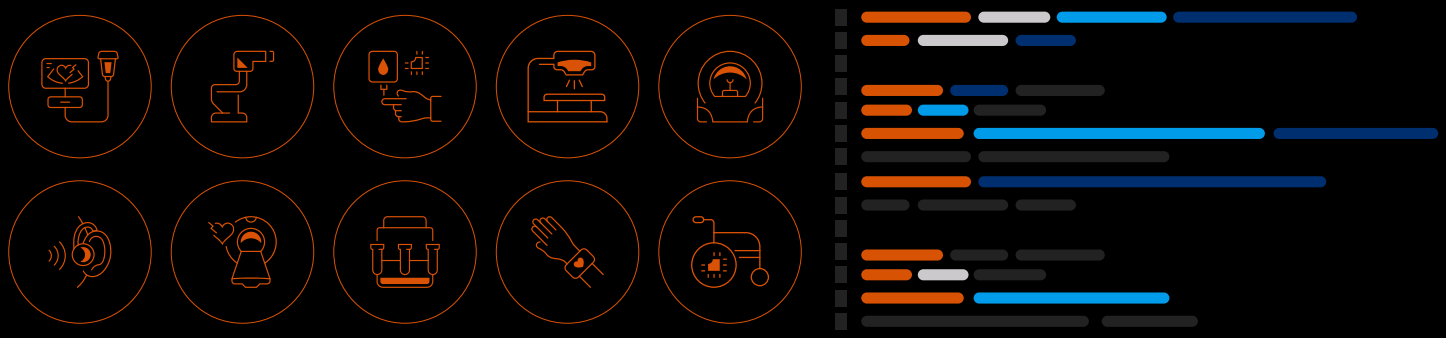
VEDERE LABS

CyberMDX
A FORESCOUT COMPANY

Access:7

How Supply Chain Vulnerabilities Can Allow Unwelcomed Access to Your Medical and IoT Devices

Table of Contents



CyberMDX Research – Now Inside Vedere Labs

The Access:7 vulnerabilities were originally discovered by the CyberMDX research team prior to the company being acquired by Forescout on Feb. 1, 2022. CyberMDX's research team is now part of Forescout's threat intelligence and research team Vedere Labs. For Vedere Labs, the combination of expertise in IT, OT, IoT and now IoMT vulnerabilities is unmatched in the industry.

Both teams had been working together to address the full impact of this disclosure for months. The two teams collaborated on identifying the list of vendors impacted by Access:7. The extensive experience of CyberMDX's 15 IoMT vulnerability discoveries, combined with those gained by Vedere Labs' prior efforts, including Project Memoria, are dedicated to serve customers and cross-industry communities with valuable data and insights aimed to keep all of us informed and safe.

1. Executive Summary

- Vedere Labs and CyberMDX have identified 7 vulnerabilities affecting the PTC Axeda agent, which we are collectively calling Access:7. Exploiting these vulnerabilities, attackers with network access to a target device could remotely execute code, access its file system or alter system configurations.
- The Axeda solution enables device manufacturers to remotely access and manage connected devices. The use of the affected agent is popular in the healthcare sector, but is also present in other industry verticals, such as financial services and manufacturing.
- A detailed list of 150+ potentially affected devices from 100+ vendors highlights the significance of the vulnerabilities. The list contains several medical imaging and laboratory devices.
- In 2014, Axeda was acquired by PTC. Upon identifying the vulnerabilities in 2021, Vedere Labs & CyberMDX collaborated with PTC to report the issues to CISA, H-ISAC and the FDA, making sure that the affected manufacturers or providers were also notified and given the opportunity to remediate before the public disclosure.
- Mitigations for device manufacturers include updating the Axeda agents, blocking numerous TCP ports and using a secure configuration. Network operators using affected devices should ensure that manufacturers are applying mitigations on their devices.

For a full list of the affected devices, visit our website (subject to change).

INFORMATIONAL

Remote servicing and its security impact

One of the main advantages of connecting a computing device to the network is being able to manage it remotely for updates, remote operation, or general servicing. Nowadays, many types of devices are remotely managed and that is usually done by someone within the organization that owns the device. There are cases, however, where the device manufacturer or another third-party are the ones performing the service.

Daily, device manufacturers and managed service providers remotely access assets deployed in facilities worldwide to help expedite their services. In some cases, this approach is adopted for efficiency and convenience. In other cases, this is a necessity for business continuity, such as in healthcare during times where COVID-19 limits service personnel from entering hospitals.

As often happens in cybersecurity, the issues here begin with lack of awareness and information. Device owners may not know when devices are being serviced, what can be done through such service, how much control is given remotely, whether there is access to sensitive information and, even more, which devices in their network are remotely serviced.

Beyond the awareness issues, there were actual vulnerabilities reported and exploited recently in remote servicing solutions. The most notorious was the Kaseya hack, where attackers exploited a vulnerability on the Kaseya VSA remote servicing solution to deploy ransomware on thousands of organizations. The Jamf management solution for macOS was also found vulnerable and SolarWinds Orion (although technically a monitoring, not a management, tool) was used to breach several US federal agencies. Other IT remote management tools like TeamViewer and NetSarang have also been used in real breaches.

The common trend is that the tools above are popular in IT environments. In the IoT world, other tools are used for very similar purposes.

IoT devices use a wide variety of operating systems, hardware and software. Typically, IoT manufacturers do not allow customers to install software, including security agents, on their devices. In the case of Access:7, PTC depends on IoT manufacturers to install the Axeda agent before their IoT devices are sold to customers in what is typically called an original equipment manufacturer (OEM) approach.

Vedere Labs and CyberMDX are constantly looking for vulnerabilities that could leave devices exposed to cyber threats as in the case of Project Memoria or ICSMA-20-343-01, aka MDHex-Ray.

MDhex-Ray disclosed 104 different radiology models (such as MRIs, CTs, X-Rays, ultrasounds and more) that are remotely serviced in an insecure way, using deprecated unsafe protocols and hard-coded passwords. Although intended to only be utilized by the manufacturer, the serviced devices were configured in a way that allowed actors from within the network to establish a service connection.

The Access:7 vulnerabilities described in this report also affect agents used for remote servicing. The difference with respect to MDhex-Ray is that Access:7 affects a solution sold to device manufacturers that did not develop their in-house remote servicing system. This makes it a supply chain vulnerability and hence it affects many downstream manufacturers and devices.

2. Main Findings

2.1. The Axeda Solution

The Axeda solution enables device manufacturers to establish connectivity to remotely monitor, manage and service a wide range of connected machines, sensors, and devices. The solution consists of a platform, agents, and assets, as shown in Figure 1:

- The platform is the server communicating with the agent. Some platforms only serve devices belonging to a specific manufacturer, whereas others serve multiple manufacturers. Most platforms are managed by Axeda, although some are managed by their manufacturer. Most platforms are deployed in the cloud, and a few are on premise.
- Agents send telemetry to their platform and receive service, depending on their configuration. An agent can represent the Asset where it is installed or be placed at a gateway and represent multiple Assets residing behind the gateway.

Service personnel from device manufacturers can also connect to a platform, through which they can read the telemetry from devices and remotely service them.

For a full list of the affected devices, visit our website (subject to change).

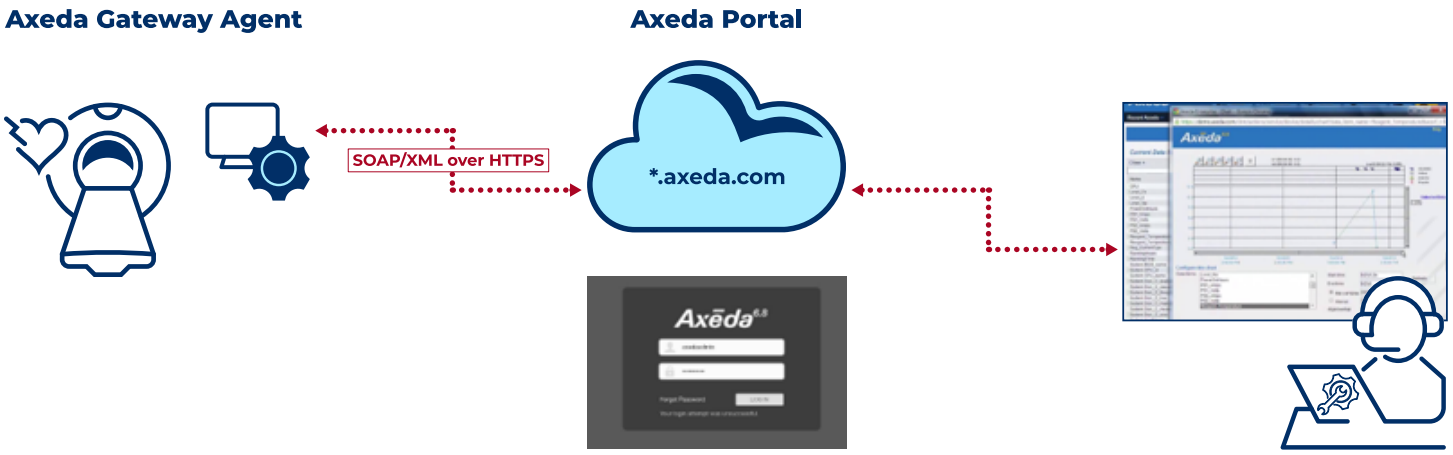


Figure 1 – Axeda solution components

Device manufacturers using the Axeda solution receive a deployment kit, which they use to generate a configured agent installation for a product line. Agents can be generated to support either the Windows or Linux operating systems, depending on the asset they run on.

2.2. Why Research Axeda

Axeda was acquired by PTC in 2014, which at that time already had more than 150 device manufacturers using this solution. Most of these were medical device manufacturers, however there was also some presence in financial services, manufacturing, and other sectors.

In 2016, BD reported a cyber incident where Axeda agents running on legacy CareFusion devices were communicating with an expired domain that had been purchased by malicious actors. That showed there was an interest of cyber attackers in remote servicing solutions for healthcare.

On customer deployments, the CyberMDX solution identified open ports, insecure protocols and deprecated software fingerprints coming from devices using the Axeda agents. Following that lead, we decided to research the agent, which consists of several resources and binaries. Listed here are the ones relevant for our discussion:

- xGate is the main agent service communicating with the platform.
- AxedaDesktopServer is a service based on UltraVNC, a commercial software used for remote screen and mouse/keyboard control. This service is not enabled in every case.
- EremoteServer.exe is an essential part of the deployment kit. This should only be used by the vendor when generating a configured agent installation for a product line. However, on some cases we found this executable deployed as part of the entire agent package.
- xBase39 is a shared library used by the specified services.

2.3. Analysis and Findings

After reverse engineering and manually analyzing the agent binaries, we found the vulnerabilities listed on Table 1. All versions including 6.9.3 are affected. Working proofs-of-concept (POCs) for all the specified vulnerabilities were supplied to PTC during the disclosure process, demonstrating that these flaws are exploitable.

CVE-ID	Description	Impact	CVSSv3.1
CVE-2022-25249	The Axeda xGate.exe agent allows for unrestricted file system read access via a directory traversal on its web server.	Information Disclosure	7.5
CVE-2022-25250	The Axeda xGate.exe agent can be shutdown remotely by an unauthenticated attacker via an undocumented command.	DoS	7.5
CVE-2022-25251	The Axeda xGate.exe agent supports a set of unauthenticated commands to retrieve information about a device and modify the agent's configuration.	RCE	9.4
CVE-2022-25246	The AxedaDesktopServer.exe service uses hard-coded credentials to enable full remote control of a device.	RCE	9.8
CVE-2022-25248	The ERemoteServer.exe service exposes a live event text log to unauthenticated attackers.	Information Disclosure	5.3
CVE-2022-25247	The ERemoteServer.exe service allows for full file-system access and remote code execution.	RCE	9.8
CVE-2022-25252	All Axeda services using xBase39.dll can be crashed due to a buffer overflow when processing requests.	DoS	7.5

Table 1 – Description of the vulnerabilities found on the Axeda agent. Rows are colored according to the CVSS score: yellow for medium or high and red for critical.

Below is a more detailed description of each vulnerability.

CVE-2022-25249: File system read access via web server

The xGate service serves HTTP and HTTPS on ports 56120 and 56130, respectively. The web server can be used to read the content of any file on the disk (provided that the service has permission to read it).

The server uses path "`Gateway/WebPages`" as its base directory and directory traversal can be used to navigate through other parent local directories and access sensitive files. For example, attackers can obtain a private key file that comes with the agent or recent backup of the system registry.

CVE-2022-25250: Shutting down the xGate.exe service

The xGate service allows a short set of commands to be sent to the engine via port 3011, including shutting it down. Establishing a connection is possible with no credentials.

CVE-2022-25251: Retrieving information about the device and modifying the agent's configuration

The xGate service supports XML-based messages over port 3031. The actions supported are the following: change configuration (such as platform hostname, encryption and others), request a status regarding platform connection establishment, read the configuration, request device info, and set the date.

CVE-2022-25246: Full remote control is protected by a hard-coded password

The AxedaDesktopServer service pulls its configuration from a local file named AxedaDesktop.ini, which is the equivalent of file ultravnc.ini on UltraVNC. Among other configurations, AxedaDesktop.ini keeps the credentials for establishing a VNC session.

The credentials are set during the deployment process by the vendor, and were found to be the same across a whole product line for a vendor.

The credentials are kept in an encrypted form. However, it uses a symmetrical encryption with a key globally used by UltraVNC, which makes the decryption straight-forward.

Establishing a VNC session is possible using a VNC client through port 5920, or using a browser through port 5820 (these are the defaults, but port number may differ per configuration).

CVE-2022-25248: Live event text log accessible

The ERemoteServer service supplies a live textual feed of the event log of this service with no authentication required via port 3077.

CVE-2022-25247: Full file-system access and remote code execution

The protocol supported by the ERemoteServer service over port 3076 supports the following actions: download a file to the device, upload a file from the device, run program, query directory/file information, shutdown ERemoteServer, shutdown xGate, and retrieve the version of the Axeda agent.

CVE-2022-25252: Crashing the agent

All services using xBase39.dll can be crashed with a malicious request. Receiving a buffer size impossible for allocation, function `SetSize` for `EByteArray` does not perform sanitization and proceeds to calling `operator_new` from `msvcr110.dll` which throws an exception. The services using this function do not handle the exception, which leads to crashing the process. Specifically, sending a too large XML size description for the xGate over port 3031 will trigger this flow and crash the xGate service. There are several more flows run by the agent's services that are similarly affected.

INFORMATIONAL

The Disclosure Process

Disclosing supply chain vulnerabilities is a notoriously long and complex process because of the number of vendors and devices affected. This is especially true for healthcare devices, since they are critical and take a long time to patch and certify.

The disclosure process for Access:7 took 210 days from initial report to public disclosure. For a reference, this is more than twice the industry-accepted 90 days limit (used, for instance, by Google Project Zero).

CyberMDX reported the vulnerabilities to PTC on the 10th of August 2021. In addition to the initial report, as per PTC's request, we have supplied working proof of concepts for exploitation and other material.

CISA was notified and approached by PTC at the beginning of November 2021, to start coordinating the process. PTC started notifying downstream vendors in January 2022. PTC was able to notify only active customers.

Being familiar with medical devices running unpatched or deprecated software, we assumed there were devices in the field from "inactive" PTC customers running this agent that should also be notified. We then decided to populate a list of vendors and products that are using or have used Axeda at some point.

Immediately after PTC and CISA agreed to our request for involving the H-ISAC, we quickly reached them to communicate the advisory to all potentially affected medical vendors from our list. A session was hosted by H-ISAC at the end of January to help vendors with technical questions and further communication was established afterwards.

FDA was consulted on the vulnerabilities at the beginning of February 2022. The public disclosure took place on the 8th of March 2022.

3. Attack Scenarios Leveraging Access:7

Access:7 includes information disclosure, denial of service and remote code execution vulnerabilities that can be used by malicious actors to achieve different goals based on their motivations, such as to gain initial access to a network via exposed vulnerable devices, exfiltrate sensitive data, or deny patient care. Below, we discuss three possible impact scenarios enabled by Access:7:

- **CVE-2022-25249:** An attacker may gain read access to the affected device's file system. The affected device, being an imaging or lab device contains sensitive information such as protected health information (PHI) or diagnostics results of a group of patients. The attacker could then profit from their finding by selling it on black markets or demanding a ransom not to do so.
- **CVE-2022-25246:** The password used for a VNC connection is the same across all models or model families for a vendor. Hence, given that attackers obtain this password they are now able to use it with any instance of the device. The password might be obtainable by purchasing a device and inspecting it, downloading an agent installation from the vendor or perhaps for some passwords they might be available publicly on the internet. In addition to the consequences described in the first scenario, the VNC connection would allow an attacker to alter information, which might be followed by patient mistreatment or denial of care. Also, running malicious code is possible and could lead to attackers persisting on the network.

- **CVE-2022-25250:** An attacker might decide to repeatedly shutdown the agent on a device, preventing it from accepting remote service when required. After a period of time, this could prevent the hospital from giving therapy or diagnosing a patient.

The attacks above require a malicious actor to be able to reach the target devices on the network, but given the nature of the healthcare sector, there are lots of attack vectors available for initial access:

- The facilities are open to the public, with some connected devices and network sockets physically accessible. In places that lack proper segmentation, attackers might also be able to access the internal operational network through a guest WiFi network.
- The medical staff can be tricked into providing initial access via phishing through e-mail addresses that are easily obtainable or by accepting imaging results on malware-infected removable media.
- IT systems can present vulnerabilities that lead attackers to the operational network. For instance, some facilities have an internet portal for scheduling appointments or viewing results. There are also systems connecting different hospitals to share medical records and test results. An attacker might be able to access the internal network on places lacking proper segmentation with the internet portal or sharing system.

4. Impact

In this section, we estimate the impact of Access:7 using information from deployments of the CyberMDX and Forescout platforms as well as public information. We have populated a list of more than 100 vendors and 150 devices that use the Axeda solution. Using Forescout Device Cloud anonymous customer data, we have seen more than 2000 unique devices running Axeda on customer networks. Examining these sources, we could better learn about the potential impact of the vulnerabilities.

4.1. Industry verticals using Axeda

Figure 2 illustrates the distribution of device vendors using Axeda. More than half of those (55%) belong to the healthcare industry, followed by almost a quarter (24%) developing IoT solutions, 8% on IT, 5% on Financial Services, 4% on Manufacturing and 4% on other verticals.

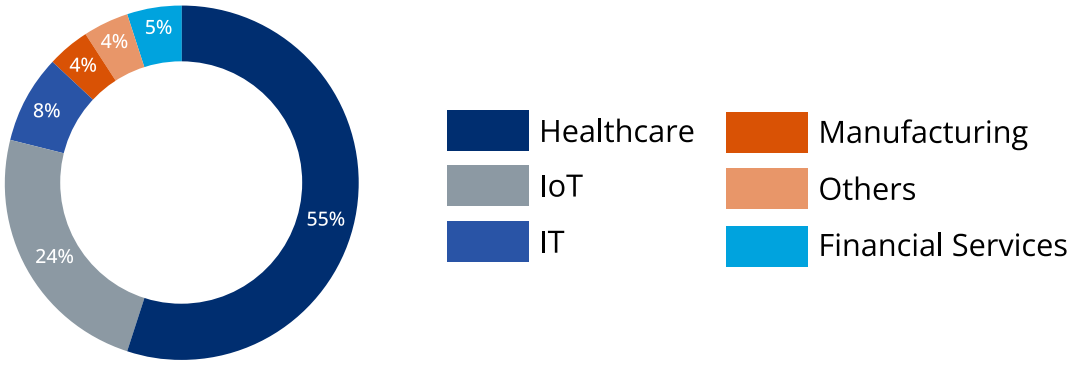


Figure 2 – Distribution of vendors using Axeda by industry vertical

This distribution is reflected on our customer deployments with devices running Axeda, which is shown in Figure 3. There, we again see more than half of the devices (54%) running in healthcare customers.

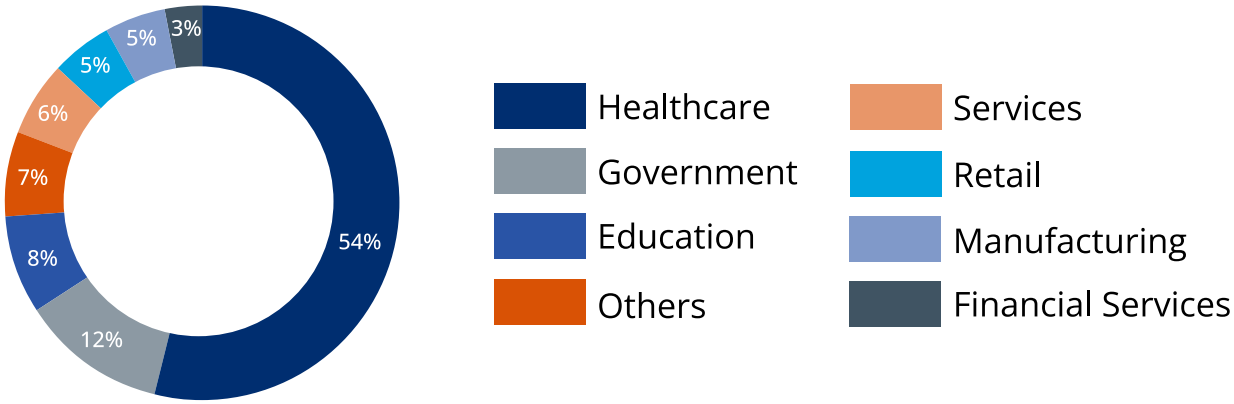


Figure 3 – Distribution of devices running Axeda on customer deployments per industry vertical

The Axeda solution was not healthcare-specific; however the largest portion of the adoption for it was in that sector. To further understand that, we proceeded to examine which types of devices in healthcare are affected.

4.2. Impact in Healthcare

Figure 4 illustrates the distribution of medical device types running Axeda. The agent was found popular in imaging and lab machines more than any other type (around two thirds of devices are in these categories). This makes sense for several reasons:

- These are the diagnostic backbones of the hospital and critical to its operation.
- They are irreplaceable, not redundant (single instances, not a fleet).
- The machines (or their adjacent control workstation) typically run under Windows or Linux which are both compatible with the Axeda agent, whereas other medical devices would usually run an embedded operating system.

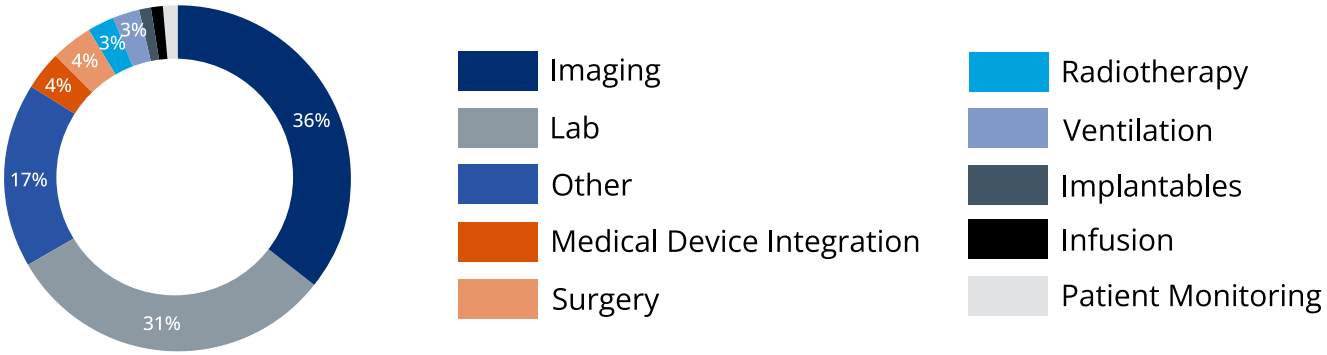


Figure 4 – Distribution of healthcare device types using Axeda

Whether using the Axeda solution or not, imaging devices generate frequent traffic with vendors, as seen by CyberMDX sensors deployed at hospitals. The most frequent traffic is telemetry reporting about the health of the device - workload, disk drives, memory consumption, failures and errors, and so on. Other less frequent sessions can originate from the outside by service personnel for addressing specific issues.

4.3. Impact in Other Industries

Axeda was developed as a cloud platform for IoT devices, therefore it is natural that there are a variety of applications beyond the healthcare industry. We did not present a quantitative chart for other industries as in the healthcare case because it would be very fragmented. There is not one or a few applications that are much more popular than others.

Nevertheless, we can mention several types of vulnerable devices that are used in these industries:

- In the financial services vertical, major ATM manufacturers used Axeda for remote management and the issue with hardcoded passwords was known (but never assigned a CVE) since 2016.
- In retail shops, there are vending machines, cash management systems, label printers and barcode scanning systems that use or have used Axeda.
- In manufacturing plants, there are vulnerable SCADA systems, asset monitoring and tracking solutions, IoT gateways and machines such as industrial cutters.

5. Mitigation Recommendations

Complete protection against Access:7 requires patching devices running the vulnerable versions of the Axeda components. PTC has released its official patches and device manufacturers using this software should provide their own updates to customers. Below, we discuss mitigation strategies for device manufacturers and network operators.

5.1 Recommendations for Device Manufacturers

1. Upgrade to Axeda agent version 6.9.1 build 1046, or 6.9.2 build 1049, or 6.9.3 build 1051 if running an older version of the Axeda agent. PTC customers can refer to https://www.ptc.com/en/support/article/CS363561
2. Configure Axeda Agent and ADS Service to only listen on the localhost interface 127.0.0.1 and prevent exposing those ports to the network. Refer to PTC Knowledge Article https://www.ptc.com/en/support/article/CS360255.
3. Provide a strong unique password in AxedaDesktop.ini file for each unit.
4. Never use ERemoteServer.exe in production
   a. Make sure to delete the ERemoteServer.exe file from the host device.
   b. Remove the installation file, for example: Gateway_vs2017-en-us-x64-pc-winnt-vc14-6.9.3-1051.msi.
   c. Also, remove any deployment utility installation and/or any other unnecessary executable files.
5. In cases where your host is using the Windows operating system, configure Localhost communications (127.0.0.1) between ERemoteServer.exe and Axeda Builder. Refer to PTC Knowledge Article https://www.ptc.com/en/

support/article/CS360255.

6. In cases where your host is not running under Windows, you'll have to run ERemoteServer.exe on a different machine. Make sure only trusted hosts can reach ports 3076, 3077 of the machine running ERemoteServer.exe.
7. Configure the Axeda agent for the authentication information required to log in to the Deployment Utility. Refer to PTC Knowledge Article https://www.ptc.com/en/support/article/CS360255.

5.2 Recommendations for Network Operators

1. Discover and inventory devices running Axeda. A constantly update list of affected device models can be found here.
2. Enforce segmentation controls and proper network hygiene to mitigate the risk from vulnerable devices. Restrict external communication paths and isolate or contain vulnerable devices in zones as a mitigating control if they cannot be patched or until they can be patched. In particular, you may consider blocking one or more of the vulnerable ports listed on Table 2, for use on any of the affected devices in your organization. The port numbers are listed here with their default values, note however that those can be configured differently by manufacturers.

CVE-ID	Port Numbers	Description
CVE-2022-25249	56120, 56130	Web server of main agent service
CVE-2022-25250	3011	Main agent service shutdown signal
CVE-2022-25251	3031	Main agent service configuration
CVE-2022-25246	5920, 5820	VNC agent
CVE-2022-25248	3077	Event log, used in deployment configuration
CVE-2022-25247	3076	Code execution and file system access, used in deployment configuration

Table 2 - Summary of ports affected by each vulnerability

3. Monitor progressive patches released by affected device manufacturers and devise a remediation plan for your vulnerable asset inventory, balancing business risk and business continuity requirements.
4. Monitor all network traffic for malicious packets that try to exploit these vulnerabilities. You should block known malicious traffic, or at least alert its presence to network operators.

6. Conclusions and Takeaways

Software components implementing remote service capabilities are very interesting targets for cyber attackers, especially when they are widely adopted, because they tend to allow for complete control of affected devices.

Vedere Labs identified seven vulnerabilities in a remote servicing solution called Axeda, currently owned by PTC. These vulnerabilities allow hackers to fully compromise affected devices, which are present in several industry verticals, but are especially popular in healthcare.

We believe that the distribution of Axeda agents found across industry verticals is evidence that medical devices are being remotely serviced more often than other types of devices. This research also shows that several medical device vendors chose to adopt a third-party solution for servicing operations instead of developing this capability in-house.

This research is further proof that vulnerabilities in supply-chain components tend to become very widespread and are difficult to eradicate, something we had initially observed with Project Memoria. Hopefully, our findings will drive more attention to supply chain remote servicing solutions and help to uncover similar issues in other solutions.

Vedere Labs will follow the developments of the discussed vulnerabilities and if required release updated advisories. We will also continue looking for impactful vulnerabilities in medical devices, caused by remote servicing, supply chain components or any other source, to improve the cybersecurity of the healthcare sector.