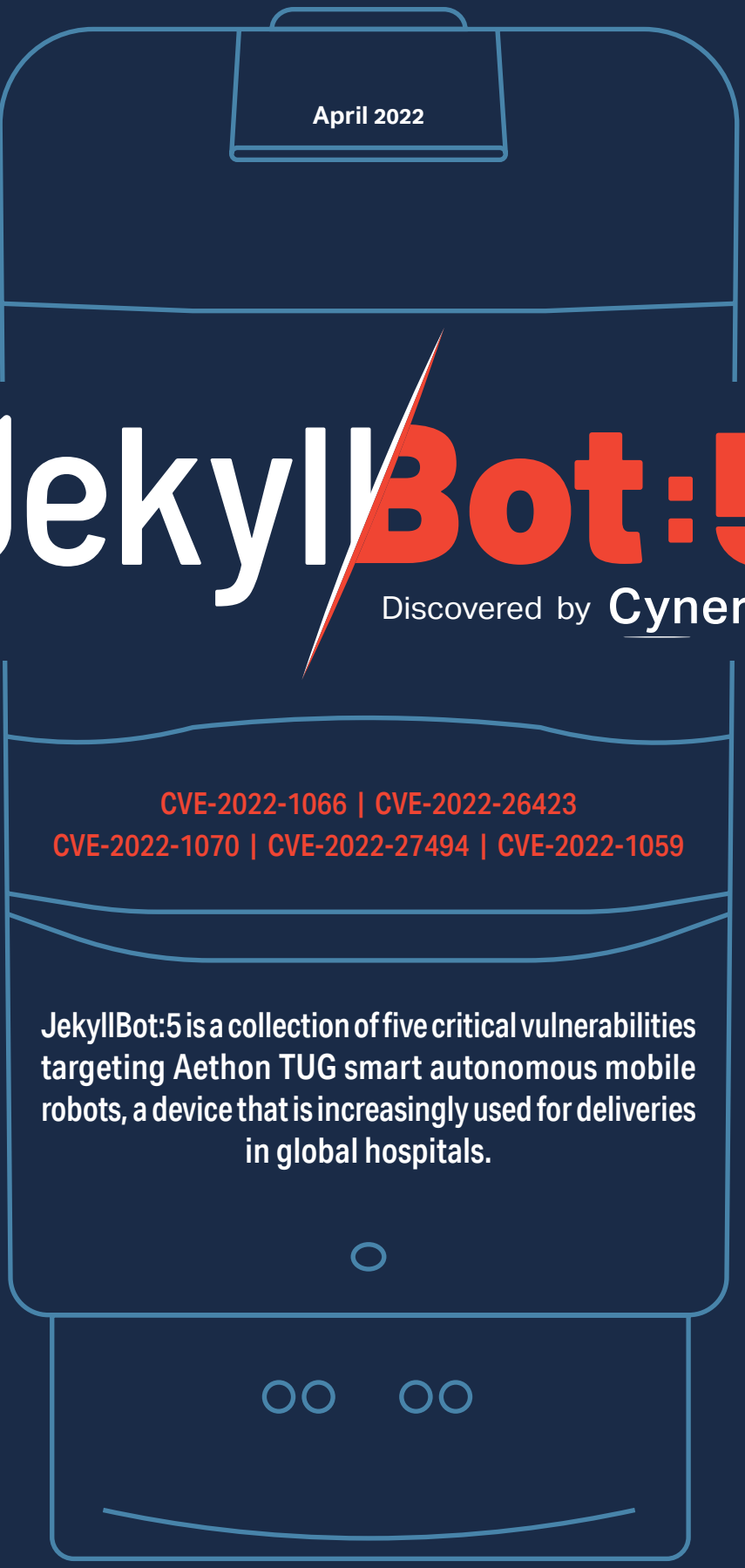
April 2022

JekyllBot:5

Discovered by Cynerio

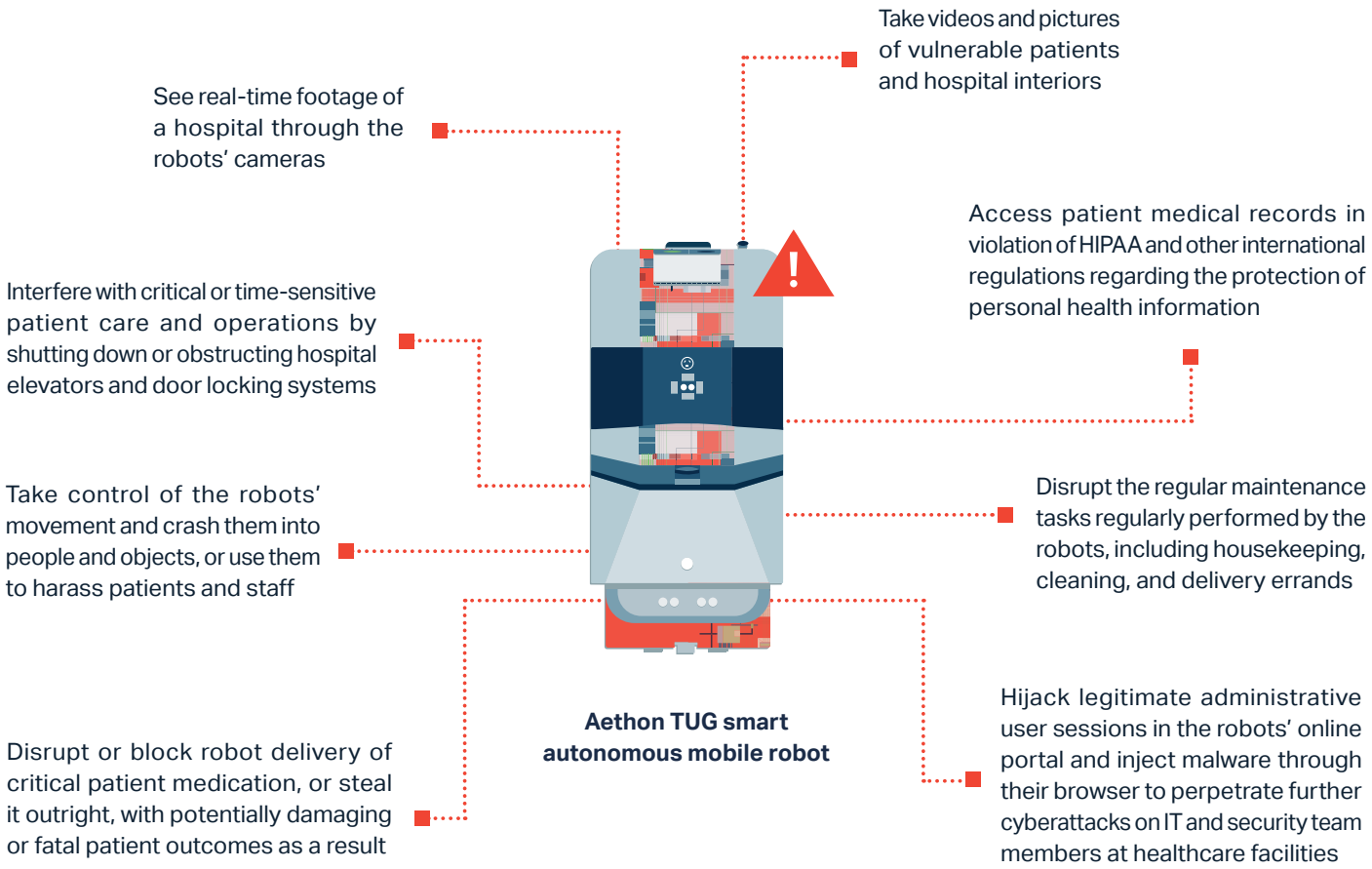
CVE-2022-1066 | CVE-2022-26423
CVE-2022-1070 | CVE-2022-27494 | CVE-2022-1059

JekyllBot:5 is a collection of five critical vulnerabilities targeting Aethon TUG smart autonomous mobile robots, a device that is increasingly used for deliveries in global hospitals.



Executive Summary

Aethon TUG smart autonomous mobile robots are used at hundreds of hospitals to deliver medicines and hospital maintenance supplies and perform simple manual labor tasks. They may sound like something out of a science fiction future, but technology has advanced to the point where semi-autonomous robots like Aethon TUGs can carry out uncomplicated errands for hospitals in a cost-effective manner while helping to optimize patient care outcomes. However, these robots require a lot of sensitive data and freedom of movement to be able to carry out their jobs effectively. JekyllBot:5 is a set of 5 critical zero-day vulnerabilities that were found by the Cynerio Live research team that enable remote control of Aethon TUG smart autonomous mobile robots and their online console. JekyllBot:5 allows attackers who exploit these vulnerabilities to:



Aethon TUG smart autonomous mobile robot

Complete detailed technical information about the risks presented by the JekyllBot:5 vulnerabilities, including which exploit mechanisms were leveraged and how to effectively mitigate potential attack scenarios, can be found within the body of this report.

Cynerio

The following table presents a summary of the Aethon TUG Base Server vulnerabilities publicly disclosed by Cynerio that have been fixed for all versions before version 24.

CVE ID	CVSS Score	Description	Potential Impact
CVE-2022-1066	8.2	The software does not perform an authorization check when an actor attempts to access a resource or perform an action.	An unauthenticated attacker can arbitrarily add new users with administrative privileges and delete or modify existing users.
CVE-2022-26423	8.2	The software does not perform an authorization check when an actor attempts to access a resource or perform an action.	An unauthenticated attacker can freely access hashed user credentials.
CVE-2022-1070	9.8	The product does not adequately verify the identity of actors at both ends of a communication channel, or does not adequately ensure the integrity of the channel, in a way that allows the channel to be accessed or influenced by an actor that is not an endpoint.	An unauthenticated attacker can connect to the TUG Home Base Server websocket to take control of TUG robots.
CVE-2022-27494	7.6	The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.	The “Reports” tab of the Fleet Management Console is vulnerable to stored cross-site scripting (XSS) attacks when creating or editing new reports.
CVE-2022-1059	7.6	The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.	The load tab of the Fleet Management Console is vulnerable to reflected cross-site scripting (XSS) attacks.

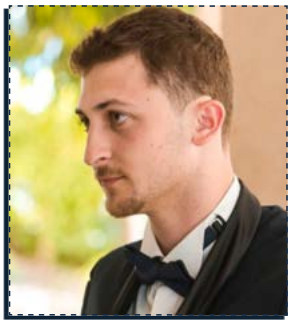
Table Of Contents

About Cynerio and the Cynerio Live Research Team

The growing number of connected medical devices in hospital networks has introduced a new breed of threats that healthcare organizations cannot address with traditional IT cybersecurity solutions. Cynerio seeks to give healthcare security teams full control over the security of their IoT, OT and IoMT ecosystems, ensuring data protection, service continuity and patient safety.

The Cynerio Live research team is made up of a number of ex-members of Unit 8200 in the Israeli Intelligence Corps, the intelligence arm of the Israeli military responsible for collecting signal intelligence and code decryption. They are roughly equivalent to the National Security Agency (NSA) in the US or the Government Communications Headquarters (GCHQ) in the UK. Unit 8200 is primarily staffed by 18-21 year-old Israeli army conscripts that are recruited for their computer science, coding and hacking skills. Many Unit 8200 alumni have gone onto successful careers in cybersecurity and technology once their service is finished.

Daniel Brodie, co-founder and CTO of Cynerio, is a Unit 8200 alum that worked on research projects that won the Israel Defense Prize, which is given to people and organizations that are deemed to have made significant contributions to Israel's self-defense. After he completed his service he went on to a career leading cybersecurity research at companies such as Lacoon, Metapacket, and Checkpoint. While at Lacoon, his team was the first security research team to be able to link specific strains of malware to the Chinese government efforts to spy on protests in Hong Kong.



Lead researcher on this project **Asher Brass** is also a fellow Unit 8200 alum, having served as an intelligence analyst and cyber intelligence team leader in the unit. He has also worked as a technological intelligence officer and researcher at the Israeli Prime Minister's Office. He specializes in vulnerability research, network analysis, and the Cyber-SIGINT domain.

Brodie and Brass are a part of the broader Cynerio Live research team that investigate the latest threats and vulnerabilities to healthcare IoT devices and help develop ways to mitigate and remediate the risks they present to patient safety, care and data. Earlier this year, the Cynerio Live team analyzed data collected from millions of IoT and IoMT devices from Cynerio deployments at hospitals in the United States and around the world as part of a report on the risks, threats and security issues associated with healthcare IoT. The first-of-its-kind report included hard numbers about the types of connected devices hospitals tend to have, the critical risks those devices contain, and how to best protect them as threats and attacks continue to evolve.

Quick Links About Cynerio

About Cynerio and Leadership

Cynerio's Website

Cynerio's Research on IoMT Vulnerabilities

About Aethon TUG Smart Autonomous Robots

Aethon was founded in 2001 and released its first TUG robot on the market in 2004. One of their principal use cases is for hospitals, and they are programmed to handle common healthcare-related tasks such as transporting medicine, cleaning floors, collecting meal trays, and many other similar errands.

TUG robots move all over the hospital, can hold up to hundreds of pounds of load at a time, interact with patients, and handle many important clinical medications and supplies. To carry out their tasks, the robots leverage several common communication protocols, including radio waves that help them to open doors, network-interface panels that allow them to go up and down elevators without human assistance, and cameras and motion sensors that help them to avoid bumping into objects and people. Because of these sensors, they don't need to use magnets, painted floor lines, or other crude methods of navigation. They can also be programmed to use a limited vocabulary that permits them to greet and communicate with people about their tasks.

Tugs Now Operate In Hundreds of Hospitals, and There Are Thousands Of Aethon Tug Robots Currently In Operation Across North America, Europe and Asia.

About three years ago, Aethon also introduced several lines of autonomous robots designed for the hospitality sector, and they have been adopted by major hotel chains such as Sheraton for simple room service, housekeeping and bellhop errands.

An example of an Aethon TUG robot. Source: aethon.com

How Cynerio Found JekyllBot:5

The Cynerio Live research team has discovered 5 vulnerabilities targeting Aethon TUG autonomous robots, collectively known herein as "JekyllBot:5." Cynerio Live discovered the vulnerabilities while carrying out a deployment for a customer hospital. Aethon TUG robots communicate over Wi-Fi, which must be converted to ethernet when the fleet management system is accessed. Late last year, a Cynerio Live researcher detected anomalous network traffic that seemed to be related to the elevator and door sensors. That in turn led to an investigation that revealed a connection from the elevator to a server with an open HTTP port, which then gave the researcher access to a company web portal with information about the Aethon TUG robots' current status, hospital layout maps, and pictures and video of what the robots were seeing. Subsequent research revealed that control of the robots was also possible through this unauthorized access. Further digging revealed some basic HTML vulnerabilities on the Aethon TUG web portal page that affect any authorized user logging into it. The vulnerability allowed an attacker to insert malicious javascript code on the report requester's browser whenever they logged in. This would allow attackers the ability to inject malware on any computer seeking to obtain data about Aethon TUG robots.

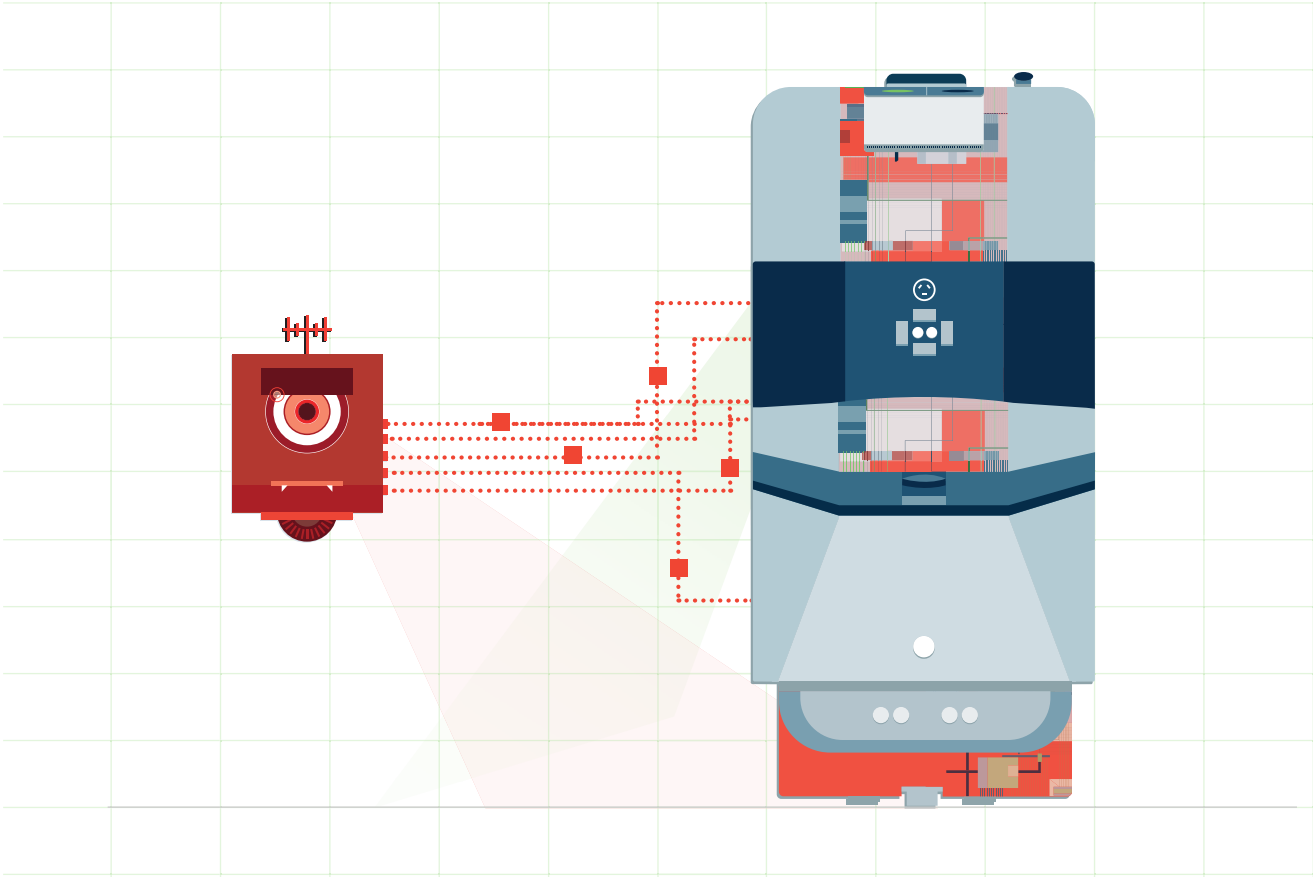
Cynerio immediately and directly notified the affected hospital so they could protect themselves, and also notified the manufacturer through the US Cybersecurity and Infrastructure Security Agency's (CISA) online Coordinated Vulnerability Disclosure (CVD) process. Thankfully, the customer who had these Aethon TUG robots in their hospital did not have them connected to the internet. But our research team felt certain that hospitals somewhere must, and found several hospitals in the United States and around the world utilizing these robots with an enabled internet connection, and in each case could leverage the vulnerabilities to control those robots directly from the Cynerio Live research lab. These additional hospitals were subsequently notified. Some of our demo exploits and descriptions of each potential attack scenario based on the vulnerabilities we discovered are covered below. **Cynerio has worked closely with Aethon, the manufacturer of these robots, to ensure that the latest version of the robot firmware contained patches and fixes for each vulnerability the Cynerio Live research team found before any public reporting.**

JekyllBot:5 Vulnerabilities and Attack Scenarios

Aethon TUG robots are able to access otherwise restricted areas of the hospital where most people can't go, including elevators and hallways secured by door-locking systems, and to retrieve medications and other sensitive materials most people can't obtain. A diverse collection of sensors and cameras enables them to move around a hospital without a lot of human intervention needed and they can autonomously direct themselves without bumping into anything or anyone.

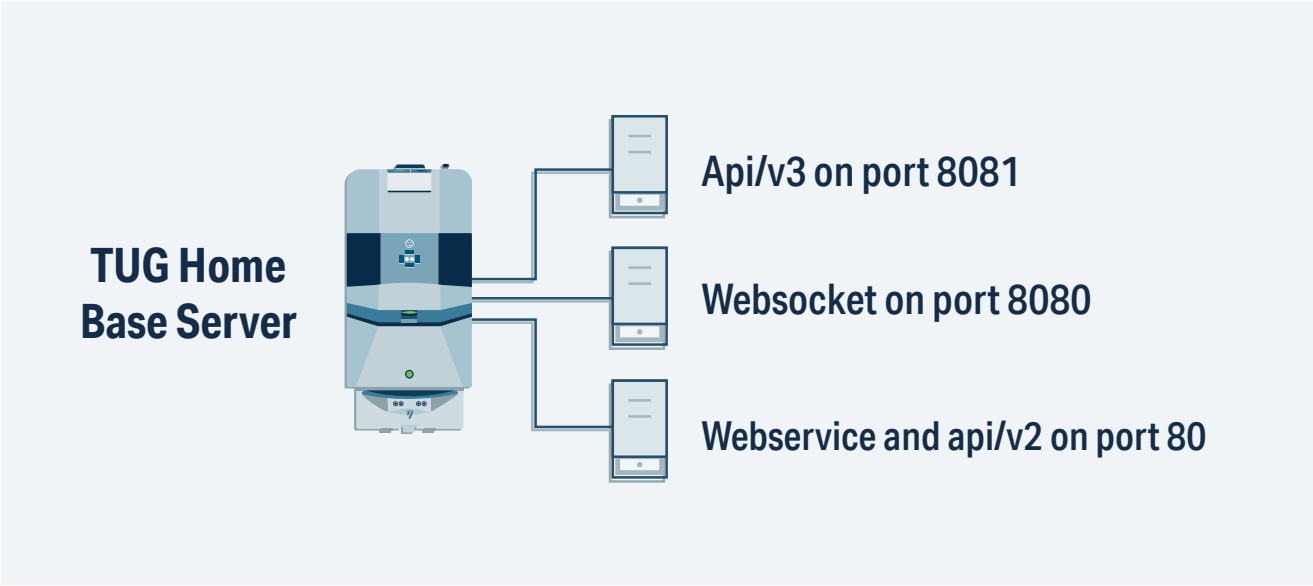
However, Cynerio researchers found that these very sensors and cameras could potentially be manipulated by attackers through multiple vulnerabilities that allow them to gain unauthorized access to the robots' command and control console, get full control of the robot fleet's movements and actions, directly interfere with patient care and data, and inject malware into legitimate user devices utilized to access the console.

The JekyllBot:5 vulnerabilities resided in the TUG Homebase Server's JavaScript and API implementation, as well as a websocket that relied on absolute trust between the server and the robots to relay commands to them. This highlights the major security issue that was at the core of the robots' operating system exposed by the vulnerabilities: the security components underpinning Aethon TUG devices were located in the JavaScript that was running in the browser of the user connected to their portal. **This meant that all security measures in place for these devices could be bypassed, and that every action Cynerio researchers subsequently tested was not validated or checked by the system.** The attack scenarios laid out in more detail below all flowed from this fundamental flaw.



The vulnerabilities impacted all versions of the robots prior to version 24, and pose a significant risk to all of the impacted Aethon TUG robots that have not been updated or patched.

The central component of a deployed TUG robot fleet is the TUG Home Base Server. This server is in constant bi-directional communication with the individual TUG robots, elevator control panels, and the various computers where the TUG console is accessed. When accessed over http, this server is called the Fleet Management Server. The Cynerio Live team identified three different network interfaces used by the TUG Home Base Server:



If either of the latter two interfaces on the above list (80 and 8080) were open to an attacker, this could have enabled a total takeover of the system and its robots due to the vulnerabilities enumerated in this document. Blocking these ports was not enough by itself to protect against the most severe vulnerabilities that the Cynerio Live team found. Additionally, leaving port 8081 open could have led to a data breach or left an open entry point for future attacker reconnaissance. Typically this solution would be part of an internal deployment at the hospital using it, but the Cynerio Live team found several TUG Home Base Servers freely accessible over the internet. This means that all security measures for these devices would have been fairly trivial for attackers to bypass. Since the TUG Home Base Server completely trusted a user's browser, all subsequent actions carried out by unauthorized parties would not be validated. Once an attacker leveraged the "original sin" of the Aethon TUG devices' JavaScript-based flaw to give themselves unauthorized access to their portal, further exploitation would have only required the most basic of attack knowledge to carry out the following JekyllBot:5 attack scenarios:

- Investigating anomalous network traffic from an elevator led Cynerio Live researchers to a server that it was connected to with an open port. This allowed Cynerio Live to see an Aethon TUG website with information about robot status, pictures and video. A vulnerability like this potentially gives attackers a way to gain unauthorized access to patients in compromising positions, as well as their personal health data.

- Cynerio Live researchers were able to send arbitrary commands to the robots via their Homebase server. Through a rudimentary brute-force attack to determine in-place passwords, they were able to create a user that was granted Admin privileges by default, and were also able to create an ordinary authorized user through an API call who then could be defined as an Admin through privilege escalation. This then allowed Cynerio researchers to monitor the robots, peer through the robots' cameras, and even control what the robots did. Taken to extremes, this unauthorized access could have led to an attacker manipulating the robots to say unauthorized or abusive phrases to harass patients and staff, controlling or shutting down smart elevators and doors to interfere with critical patient or operations, and even altering medicine dispensation to the point where patient care and outcomes are disrupted or jeopardized. (Cynerio Live researchers didn't do most of these things – that would have been dangerous! - but once they gained access to the portal they saw exactly where all these things could be manipulated).

- By opening a websocket, Cynerio Live researchers could control the robots even without having access to their user interface. The code that allows this was fairly simple and JavaScript-based and permitted access to the robot's control mechanisms through port 8080. Since this method relied on websockets, it was not very complex - technically a hacker on the hospital network connected through a laptop could have exploited it.

- The robots had a vulnerability that permitted an attacker to inject malicious JavaScript whenever any authorized user logged into the online management console for the robots, so that when they entered the online portal, malware was injected on the user's browser that enabled credential stealing and could be used to track that user's subsequent activity.

It is important to note that these vulnerabilities could be exploited both over the network and the internet, and required a very low skill set for exploitation, no special privileges, and no user interaction to be successfully leveraged in an attack. If attackers were able to exploit these vulnerabilities, they could have completely taken over system control, denied service to legitimate users and gained access to real-time sensitive information such as camera feeds and device data.

Hospitals using Aethon TUG robots are advised to make sure their devices are patched with the latest version of the firmware to prevent potential exposure to the JekyllBot:5 vulnerabilities. Additionally, Cynerio recommends proactive measures to limit exposure to similar vulnerabilities that may yet be found, including ensuring no external internet connectivity for the Aethon TUG robots and segmenting their network location to minimize usage of the robots as entry or pivot points by potential attackers.

Our research reveals that Aethon TUG robots most likely don't allow for the installation of a security agent like an Endpoint Detection and Response (EDR) solution, and their vulnerabilities did not have any other mitigation possibility aside from new patches or a complete reconfiguration of the device operating system.

JekyllBot:5 Exploits At A Glance

In this section, we will outline the scenarios attackers could use to take advantage of JekyllBot:5 vulnerabilities.

Privilege Escalation for the Unauthenticated User

Privilege Escalation - Exploit 1

Through this vulnerability, an unauthenticated attacker could arbitrarily add new users with administrative privileges, and delete or modify existing users, via POST and PUT API calls to the following path over http:<HOMEBASESERVERADDRESS>/api/tug/v2/user/

Once an attacker successfully created a new user with administrative privileges, they could freely modify parameters relating to other users, robots, elevators, reports, and more. This would allow them to effectively control the Fleet Management Console while shutting out legitimate users.

In addition, through the user interface, the robots have a joystick module similar to a video game controller. Through this joystick module, Cynerio Live researchers saw where they could move the robots around and send them commands, including DoS attacks on smart elevators and doors. They could also see what the robot's camera sees in real time.

Privilege Escalation - Exploit 2

An unauthenticated attacker could freely access hashed user credentials via brute forced http GET requests to <HOMEBASESERVERADDRESS>/api/tug/v2/user/ and passwords were stored using md5 hashing, which could be brute forced. In our case, the password of 123456 became e10adc3949ba59abbe56e057f20f88. As with the first way to exploit this vulnerability, the joystick module allowed attackers to completely take control of a given robot to move it around and give it commands.

Complete Robot Control via an Exposed Websocket on Port 8080

An unauthenticated attacker could connect to the TUG Home Base Server websocket over port 8080 and take complete control of the TUG robots. This would have given attackers the ability to do the following:

- **Create new movement commands while controlling the robot's speed**
- **Cancel existing tasks the robot was already programmed to do**
- **Forcing a robot to ride, call or exit an elevator**
- **Turning the laser beam the robot uses for navigation on and off**
- **Docking and undocking the robot**
- **Opening and closing the drawers the robot uses to dispense medication**
- **Reporting current location**

Information Leakage via API on Ports 8081 and 80

The /api/tug/v3/ and /api/tug/v2/ methods were freely accessible over http on ports 8081 and 80, and could be used by an unauthenticated attacker to obtain real-time photos from TUG robots, obtain current robot coordinates, and other potentially sensitive information.

XSS Vulnerabilities in the Fleet Management Console

The Fleet Management Console was vulnerable to stored XSS attacks when an authorized user was logged into it. This fact, combined with the fact that the console only used a simple PHPSESSIONID cookie for session identification, could have allowed an attacker to hijack legitimate user sessions with higher privileges, or inject other malicious or arbitrary code into the browser of the user accessing the console.

JekyllBot:5 Mitigations and Fixes

The JekyllBot:5 vulnerabilities highlighted in this report have been fixed by the device manufacturer since Cynerio notified them of the risks through the CISA Coordinated Vulnerability Disclosure process. Several patches have been applied to the robot fleets at each Aethon customer hospital, including one major patch that required replacing firmware and an operating system update for robots at some hospitals. In addition, Aethon was able to update the firewalls at particular hospitals known to have vulnerable robots so that public access to the robots through the hospitals' IP addresses was prevented as the fixes were rolled out. This isolated the robots from the internet communication that would have enabled an attacker to gain unauthorized access to the robots.

Cynerio offers additional layers of protection for these and other device vulnerabilities through its detection of active exploitation attempts on a network's healthcare IoT footprint. Expedited attack and risk mitigation practices carried out by Cynerio include:

- The location and flagging of every device with known risks and vulnerabilities such as JekyllBot:5.
- Step-by-step instructional mitigation plans for each device affected by a vulnerability, including links to advisories and patches from device manufacturers and "virtual patching" options for end-of-life or otherwise unpatchable devices.
- Detailed Zero Trust policy formulation to ensure that devices are hardened or quarantined against unauthorized, unauthenticated or unverified access attempts.
- A policy engine sandbox that streamlines network segmentation options for healthcare IoT devices, allowing hospitals to monitor, test, validate and update potential segmentation policies before they are enforced so that security and network teams can confidently confirm service continuity for protected devices.

Conclusion: Cybersecurity Must Do Better for Healthcare IoT

Even with all the investment made towards effective cybersecurity on the part of hospitals, potential vulnerabilities in healthcare IoT devices still loom large, and attacks on them continue to surge, even amidst an ongoing pandemic. The cybersecurity industry as a whole has failed to keep hospitals safe, especially when it comes to the IoT and IoMT devices connected to patients, and that can't continue as ransomware attacks on healthcare continue to shatter records. Healthcare IoT security solutions that focus on years-long asset management and inventory processes before addressing device risks and live attacks are leaving hospitals exposed and enabling future attacks, and would not be able to address zero-day vulnerabilities like the ones highlighted in this research except by shutting the devices down and making them inoperable. When patient lives depend on those devices, turning them off is not an option, but neither is exposing them to attacker threats.

Identifying and addressing risks and attacks on healthcare IoT needs to be the focus of any strategy meant to curb attacks on this growing threat vector. Unfortunately, too many established approaches for healthcare IoT security use inventory as their central focus and won't advance on remediating risk or attacks until months or even years into a deployment, or not at all. As the dependency on these healthcare IoT devices and their volume exponentially grows, hospitals will need solutions that treat those devices in much the same way that IT security does, with proactive mitigation of their risks and immediate protective actions for any detected attacks or malicious activity. Any less is a disservice to patients and the devices they depend on for optimal healthcare outcomes.

Too many established approaches for healthcare IoT security use inventory as their central focus and won't advance on remediating risk or attacks until months or even years into a deployment, or not at all.

About Cynerio

Cynerio is the one-stop-shop Healthcare IoT security platform. With solutions that cater to healthcare's every IoT need – from Enterprise IoT to OT and IoMT – we promote cross- organizational alignment and provide hospitals the control, foresight, and adaptability they require to stay cyber-secure in a constantly evolving threatscape. We empower healthcare organizations to stay compliant and proactively manage every connection on their own terms with real-time IoT attack detection & response and rapid risk reduction tools, so that they can focus on a hospital's top priority: delivering quality patient care. For more information visit www.cynerio.com, or follow Cynerio on Facebook, Twitter, and Linkedin.