HC3: Alert

April 13, 2022 TLP: WHITE Report: 202204131500

ICS Advisory - Aethon TUG Home Base Server

Executive Summary

Aethon reports these vulnerabilities affect all versions prior to Version 24 of TUG Home Base Server, a server used to control and communicate with autonomous mobile robots in hospitals.

Report

ICS Advisory (ICSA-22-102-05) - Aethon TUG Home Base Server
Aethon TUG Home Base Server | CISA

Impact to HPH Sector

Aethon has implemented a mitigation plan to address these vulnerabilities. Aethon has checked all locations where this product is in use to ensure firewalls are active and to update systems to the newest software (Version 24).

CISA recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures. CISA also provides a section for control systems security recommended practices on the ICS webpage on cisa.gov.

CISA offers a range of no-cost cyber hygiene services to help organizations assess, identify, and reduce their exposure to threats, including ransomware. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors. All organizations should immediately report incidents to CISA at https://us-cert.cisa.gov/report, a local FBI Field Office, or U.S. Secret Service Field Office.

References

Autonomous robots used in hundreds of hospitals at risk of remote hijacks
Autonomous robots used in hundreds of hospitals at risk of remote hijacks | TechCrunch

Contact Information

If you have any additional questions, please contact us at HC3@hhs.gov.

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback