HMS Security Advisory

XSS in Anybus-CompactCom 30

HMSSAR-2024-05-17-001

Version	Summary of changes	Date
1	Initial release	May 17, 2024

Overview

On May 2, 2024, HMS Networks was notified by Secoore of vulnerabilities discovered in an Anybus-CompactCom 30 PROFINET device. All other Ethernet based Anybus-CompactCom 30 module from the HMS Networks brand Anybus are affected by the same vulnerability. All of the legacy products have been replaced by a new backwards compatible products.

Affected products and versions

- All Anybus-CompactCom 30 products with a web server.

Impact

The Anybus-CompactCom 30 products are vulnerable to a XSS attack caused by the lack of input sanitation checks. As a consequence, it is possible to insert HTML code into input fields and store the HTML code. The stored HTML code will be embedded in the page and executed by host browser the next time the page is loaded.

Severity / CVSS Score

The CVSS[1] severity base score is 6.3, and the associated scoring vector is CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:H/SI:H/SA:N.

Recommendations

HMS recommends that at least one of the following mitigations are implemented:

- Add password protection to all webpages served by the Anybus-CompactCom 30 module.
- Disable or add the option to allow the end-user to disable the webserver in the Anybus-CompactCom 30.
- Make sure these products are used locally within a secure network utilizing proper network infrastructure controls. This will help ensure that unused or unnecessary protocols from unauthorized sources are blocked.
- Ensure that control systems and devices are situated behind firewalls, ensuring their isolation from the corporate network.
- Replace the Anybus-CompactCom 30 module with a Anybus-CompactCom 40 module.

Furthermore, HMS suggest to follow the Cybersecurity & Infrastructure Security Agency (CISA) general recommendations. CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability. Specifically, the users should:

[1] CVSS is owned by FIRST and used by permission. https://www.first.org/cvss

- Minimize network exposure for all control system devices and/or systems and ensure that 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 that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

CISA also recommends users take the following measures to protect themselves from social engineering attacks:

- Do not click web links or open unsolicited attachments in email messages.
- Refer to Recognizing and Avoiding Email Scams for more information on avoiding email scams.
- Refer to Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks.

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 us-cert.gov. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on us-cert.gov in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Product updates

No firmware update will be released to fix this issue.

Acknowledgements

HMS thanks Vincenzo Giuseppe Colacino from Secoore for finding and notifying about the vulnerability in a controlled way.