

TLP:WHITE



NCCIC

Advisory (ICSMA-18-240-01)

Qualcomm Life Capsule

Original release date: August 28, 2018

Legal Notice

All information products included in <http://ics-cert.us-cert.gov> are provided "as is" for informational purposes. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see <http://www.us-cert.gov/tlp/>.

1. EXECUTIVE SUMMARY

- **CVSS v3 9.8**
- **ATTENTION:** Exploitable remotely/low skill level to exploit
- **Vendor:** Qualcomm Life
- **Equipment:** Capsule Datacaptor Terminal Server (DTS)
- **Vulnerability:** Code Weakness

2. RISK EVALUATION

Successful exploitation of this vulnerability could allow an attacker to execute unauthorized code to obtain administrator-level privileges on the device.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following versions of Capsule Datacaptor Terminal Server (DTS), part of a medical device information system, are affected:

- Allegro RomPager embedded web server versions 4.01 through 4.34 included in Capsule DTS, all versions affected.

3.2 VULNERABILITY OVERVIEW

3.2.1 CODE CWE-17

This vulnerability allows an attacker to send a specially crafted HTTP cookie to the web management portal to write arbitrary data to the device memory, which may allow remote code execution.

TLP:WHITE

CVE-2014-9222 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

TLP:WHITE

3.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Healthcare and Public Health
- **COUNTRIES/AREAS DEPLOYED:** Worldwide
- **COMPANY HEADQUARTERS LOCATION:** United States

3.4 RESEARCHER

Elad Luz of CyberMDX reported this vulnerability to NCCIC.

4. MITIGATIONS

Qualcomm Life reports this vulnerability does not affect any other Capsule Technologies products.

Capsule Technologies has released a firmware update to remediate this vulnerability on the "Single Board" version of the DTS, which was originally released in 2009. Capsule Technologies strongly urges all users with a Single Board version of the DTS to download the firmware from Capsule's customer portal and apply it to the affected devices following standard patching processes. Access to the customer portal can be found at the following location:

<https://customers.capsuletech.com>

Due to technical limitations, the firmware update will remediate only the Single Board version of the DTS, and will NOT remediate these other versions of DTS:

- Dual Board
- Capsule Digi Connect ES converted to DTS
- Capsule Digi Connect ES

Capsule recommends that users with any of these three versions of DTS disable the embedded webserver to mitigate the vulnerability. The webserver is only utilized for configuration during the initial deployment and is not necessary for continued remote support of the device.

Additional information regarding the affected versions of the embedded Allegro RomPager webserver included in Capsule DTS can be found at the following locations:

<https://www.allegrosoft.com/allegro-software-urges-manufacturers-to-maintain-firmware-for-highest-level-of-embedded-device-security/news-press.html>

NCCIC recommends users take defensive measures to minimize the risk of exploitation of this vulnerability. Specifically, users should:

- 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

TLP:WHITE

TLP:WHITE

devices.

NCCIC reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

NCCIC also provides a section for control systems security recommended practices on the ICS-CERT web page. 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-CERT website in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to NCCIC for tracking and correlation against other incidents.

No known public exploits specifically target this vulnerability.

Contact Information

For any questions related to this report, please contact the NCCIC at:

Email: NCCICCUSTOMERSERVICE@hq.dhs.gov

Toll Free: 1-888-282-0870

For industrial control systems cybersecurity information: <http://ics-cert.us-cert.gov>

or incident reporting: <https://ics-cert.us-cert.gov/Report-Incident?>

The NCCIC continuously strives to improve its products and services. You can help by choosing one of the below to provide feedback about this product.

TLP:WHITE