Product Security Bulletin

Title: PrisMax – Treck TCP/IP Stack (Ripple20) Vulnerabilities
Publication Date: July 30, 2020

Background

This notification provides product security information and recommendations related to security vulnerabilities in the modified Treck TCP/IP stack contained in the operating system used in the PrisMax device.

ICS Advisory ICSA-20-168-01 (https://www.us-cert.gov/ics/advisories/icsa-20-168-01) described a group of vulnerabilities present in the Treck TCP/IP stack that are referred to commonly as the "Ripple20" vulnerabilities. Green Hills Software LLC (https://www.ghs.com) incorporated a highly modified version of the Treck TCP/IP stack called GHnet v2 in the INTEGRITY operating system, which Vantive uses in its PrisMax device. Because GHnet v2 implements a modified version of the Treck TCP/IP stack, the impact of "Ripple20" on GHnet v2 and PrisMax is limited to network connectivity, which is far less severe than described in ICS Advisory ICSA-20-168-01.

Affected Products

This notification applies to customers that use PrisMax with software version 2.1.

The "Ripple20" vulnerabilities only impact customers that connect PrisMax to a secondary data management system (Electronic Medical Record (EMR) / Patient Data Management System (PDMS)) using Ethernet.

Vulnerability Details

The PrisMax (software version 2.1) device is affected by only 3 of the 19 reported "Ripple20" vulnerabilities – specifically, CVE-2020-11907, CVE-2020-11911, and CVE-2020-11914. These vulnerabilities, if exploited, could impact PrisMax only if connected to a secondary data management system (EMR/PDMS) using Ethernet.

Vantive has conducted an in-depth analysis of the above three vulnerabilities and determined their CVSSv3.1 scores in the context of PrisMax specific implementation of the GHnet v2. The highest CVSS score for the 3 CVEs is 3.1, based on the assessment that a potential attacker needs access to the local network, and that a potential attack (either Denial of Service or malicious modification of network connections) requires high attack complexity. The worst impact to the PrisMax device would be loss of network connectivity, with no impact on therapy or patient safety.

PrisMax is not affected by the following 16 reported "Ripple20" vulnerabilities: CVE-2020-11896, CVE-2020-11897, CVE-2020-11901, CVE-2020-11898, CVE-2020-11900, CVE-2020-11902, CVE-2020-11904, CVE-2020-11899, CVE-2020-11903, CVE-2020-11905, CVE-2020-11906**,** CVE-2020-11909, CVE-2020-11910, CVE-2020-11912, CVE-2020-11913, and CVE-2020-11908.

Potential Impact on Performance, Safety and Data

The “Ripple20” vulnerabilities do not impact the safety or essential performance of the PrisMax device. The vulnerabilities do not allow the user to directly access or execute remote code on the PrisMax device itself. An unauthorized user would not be able to alter treatment parameters of the PrisMax device or otherwise alter the therapy delivered by the device.

If exploited, the “Ripple20” vulnerabilities could interrupt the flow of data from the device to the EMR/PDMS or expose the device identification data that is already used in routing protocols. Exploitation of the “Ripple20” vulnerabilities would not allow any exposure of personally identifiable information (PII) or protected heath information (PHI).

Vantive has not received any reports of exploits related to PrisMax and the “Ripple20” vulnerabilities.

Mitigations & Compensating Controls

The following mitigations reduce the likelihood that the “Ripple20” vulnerabilities will be exploited:

- Physical access to the PrisMax device should be limited only to authorized users.
- Customers should maintain the cybersecurity of the hospital environment by performing the following:
    - Network segmentation
    - Firewalling each network segment, limiting inbound and outbound connections
    - Scanning for unauthorized network access

If an EMR/PDMS system is to be used with the device, customers should first verify compatibility between the two systems. Customers should identify, analyze, evaluate and control risks due to integration of PrisMax in an IT network and any subsequent changes to the IT network.

For More Information

If you observe any symptoms that are representative of these vulnerabilities, detect the source of the attack and use a firewall to block the source IP and contact your service representative immediately.

Additional resources:

https://www.us-cert.gov/ics/advisories/icsa-20-168-01
https://support.ghs.com/psirt/PSA-2020-05/

For more information:

For questions regarding cybersecurity of PrisMax or other Baxter products, contact:
global.corp.product.security@vantive.com