Honeywell
THE POWER OF CONNECTED

Cyber Security Update

Honeywell Safety and Productivity Products |

RIPPLE20 vulnerability

Publish Date: 07-17-2020
Reference: ICS-CERT Advisory ICSA-20-168-01
Severity: Some are High depending on usage

CISA's Advisory: ICSA-20-168-01

Summary

The Treck TCP/IP protocol suite is a high-performance stack designed for use in embedded systems. Security researchers have discovered 19 vulnerabilities which is collectively named "Ripple20". This protocol suite is used in a wide range of systems across many commercial and consumer products in industries including healthcare, manufacturing, telecom, energy distribution and others. The primary impact of these vulnerabilities is the potential for remote code execution and denial of service (DoS).

To date, there are no known exploits.

Honeywell strongly encourages customers to upgrade firmware on these affected devices based on the date identified below. Until these security updates are made available, Honeywell recommends implementing mitigation techniques mentioned in the section title "**Mitigating Techniques**".

Recommended Action

Honeywell will release firmware software updates to include security fixes as these are made from our partners. The following list contain those products that Honeywell Scanning and Mobility have identified as potentially affected by this vulnerability. Updates will be made available at https://hsmftp.honeywell.com, or from through your Honeywell product support channel.

Product Name	Software	Status	Comments
RL 3/4	GreenHills Int 10.0.2	Affected	Honeywell expects a patched firmware release will be available August 14, 2020
RL 3e/4e	GreenHills Int 10.0.2	Affected	Honeywell expects a patched firmware release will be available August 14, 2020
RP 2/4	GreenHills Int 10.0.2	Affected	Honeywell expects a patched firmware release will be available August 14, 2020
E-Class	GreenHills Int 10.0.2	Affected	Honeywell expects a patched firmware release will be available August 14, 2020
I-Class	GreenHills Int 10.0.2	Affected	Honeywell expects a patched firmware release will be available August 14, 2020
MP Compact MkIII	GreenHills Int 10.0.2	Affected	Honeywell expects a patched firmware release will be available August 14, 2020

A-Class	Nucleus	Affected	Honeywell expects a patched firmware release will be available August 31, 2020
H-Class	Nucleus	Affected	Honeywell expects a patched firmware release will be available August 31, 2020
M-Class	Nucleus	Affected	Honeywell expects a patched firmware release will be available August 31, 2020
PB 21/22/31/32	ThreadX	Affected	Honeywell expects a patched firmware release to be available September 15, 2020
PB 50/51	ThreadX	Affected	Honeywell expects a patched firmware release to be available September 15, 2020
PR2/3	ThreadX	Affected	Honeywell expects a patched firmware release to be available September 15, 2020
PD42	ThreadX	Affected	Honeywell expects a patched firmware release to be available September 15, 2020
PM4i	netBSD	Affected	This product will not receive a patch, we recommend customers use mitigating techniques described in this document.
PX4i	netBSD	Affected	This product will not receive a patch, we recommend customers use mitigating techniques described in this document.
PX6i	netBSD	Affected	This product will not receive a patch, we recommend customers use mitigating techniques described in this document.

Mitigating Techniques

Honeywell recommends that customers use technical controls such as network segmentation, firewalls, intrusion prevention, anomaly detection and other methods to ensure AIDC equipment such scanners, printers and mobile computers are isolated from the rest of the business network.

Honeywell also suggests customers include network monitoring for fragmented network packets, improperly structured DNS,ICMP packets, and DHCP as well as short-length network frames.

Additional security recommendations are found in the Network and Security Guide for Honeywell Printers. (https://www.honeywellaidc.com/en/-/media/en/files-public/technical-publications/printers/pc42/printer%20security%20guide%20pdf.pdf)

Product Support

For assistance with this vulnerability please contact Honeywell through your product support channel. If you become aware of a vulnerability or other security concern involving a Honeywell product, please notify Honeywell by sending an email to security@honeywell.com

DISCLAIMERS

- CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY.

- YOUR USE OF THE INFORMATION ON THIS DOCUMENT OR MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK.
- HONEYWELL RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME AND WITHOUT NOTICE.
- HONEYWELL PROVIDES THE CVSS SCORES “AS IS” WITHOUT WARRANTY OF ANY KIND. HONEYWELL DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PURPOSE AND MAKES NO EXPRESS WARRANTIES EXCEPT AS MAY BE STATED IN A WRITTEN AGREEMENT WITH AND FOR ITS CUSTOMERS