Expertise in
Turbomachinery
Optimization

Compressor Controls Corporation
4745 121st Street
Des Moines, IA
50323-2316 U.S.A.
+1-515-270-0857
www.cccglobal.com

CCC Security Advisory 2020-01

CCCSA-2020-01

Released: July 21, 2020

DISCLAIMER:

Revision #	Revision Date	Revision Description
1	July 21, 2020	Initial Release

1 Applicability

This security advisory is applicable to customers utilizing the following products:

- PRODIGY® control system (all versions released at the time of this advisory)
- Series 3++ controllers with Ethernet backplane
- Digi ConnectPort TS Serial to Ethernet Media Converter
- Intel NICs with select firmware versions on TrainTools servers (Dell, HPE, Beckhoff)

All other products including, but not limited to, Series 3 Plus, Series 3++ with Serial backplane, Series 4, Series 5, and DigiOne IA are not applicable.

2 Overview

Ripple20 is a collection of 19 security vulnerabilities discovered in TCP/IP stack developed by Treck, Inc. The Treck TCP/IP stack is utilized by a wide range of devices from network switches, Uninterruptable Power Supplies, printers, to industrial controllers. Successful exploitation of these vulnerabilities may allow remote code execution or exposure of sensitive information.

2.1 Assessed Vulnerabilities

The following is a list of 19 vulnerabilities assessed. Further information can be found on the CISA website [1] under ICS-CERT Advisory Number: ICSA-20-168-01.

- CVE-2020-11896
- CVE-2020-11897
- CVE-2020-11898
- CVE-2020-11899
- CVE-2020-11900
- CVE-2020-11901
- CVE-2020-11902
- CVE-2020-11903
- CVE-2020-11904
- CVE-2020-11905
- CVE-2020-11906
- CVE-2020-11907
- CVE-2020-11908
- CVE-2020-11909
- CVE-2020-11910
- CVE-2020-11911
- CVE-2020-11912
- CVE-2020-11913
- CVE-2020-11914

2.2 CCC Assessment

Based on our internal investigations along with the advisories issued by CCC's technology partners, we have identified a limited number of CCC products and third-party products that have been impacted.

The following CCC products include affected versions of Treck TCP/IP stack:

- PRODIGY® control system
- Series 3++ controllers with Ethernet backplane

The following third-party products may include affected versions of Treck TCP/IP stack:

- Digi ConnectPort TS Serial to Ethernet Media Converter
- Intel NICs with select firmware versions

All other products are not known to be affected at the time of this advisory's publication.

3 Mitigation

3.1 Reducing Attack Surface

In order to minimize the attack surface, customers are advised to follow the best practices recommended by CISA:

- 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.
- Use an internal DNS server that performs DNS-over-HTTPS for lookups.

Additionally:

- For PRODIGY controllers, all network interfaces of PRODIGY shall be restricted to TrainTools Server(s) to properly segregate Level 1 assets from Level 2 and Level 3 as per ISA/IEC 62443. To ensure this, customers are advised to make communication architecture assessment against *TN101 TrainTools Networks with PRODIGY Controllers* [2]. Specifically, customers are advised to investigate and document any direct connection between 3rd-party systems and PRODIGY network interfaces.
- For Series 3++ controllers with Ethernet backplane, the network shall be restricted to containing other Series 3++ controllers and intended Modbus TCP client only. This network segmentation may be either physical or virtual (VLAN).

3.2 Patching the Affected Products

CCC has worked with vendors and partners to create and qualify patches that will address these vulnerabilities. Please refer to section 4. Update Availability for further details.

4 Update Availability

Patches for the following products must be deployed offline either by or under the supervision of CCC service personnel. Please contact CCC Technical Support for further information and assistance.

https://www.cccglobal.com/contact-ccc/technical-support-form/

- PRODIGY® control system
- Series 3++ controllers with Ethernet backplane

Patches for the following third-party products may be obtained directly from their respective websites.

- Digi ConnectPort TS Serial to Ethernet Media Converter

  https://www.digi.com/support/knowledge-base/digi-international-security-notice-treck-tcp-ip-st

- Intel NICs with select firmware versions

  https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00295.html

5 Disclaimer

The information provided in this advisory is bound to the Terms and Conditions provided with the original system delivery. The latest copy of the Terms and Conditions is available at:

https://www.cccglobal.com/terms-and-conditions

6 References

[1] CISA, "US-CERT ICS Advisory (ICSA-20-168-01)," 2020. [Online]. Available: https://us-cert.cisa.gov/ics/advisories/icsa-20-168-01.

[2] Compressor Controls Corporation, "TN101 TrainTools Networks with PRODIGY Controllers".