Eaton Security Bulletin

ETN-SB-2020-1008: Multiple security vulnerabilities in Treck TCP/IP stack termed as “Ripple20”

Publish Date	Impacted Eaton Product(s)	CVE ID(s)	Severity
6/23/2020 Updated 7/15/2020 Updated 7/24/2020 Updated 8/6/2020	CL-7 voltage regulator control Form 4D recloser control Form 6 recloser control Edison Idea and IdeaPLUS relays (all variants) Eaton G3/G3+ ePDU • Metered Input PDU • Metered Outlet PDU • Managed PDU • High Density PDU Network Management Card Mini slot (NMC/Network-MS) card • Uninterrupted Power Supply (UPSs) with Network-MS card • Automatic Transfer Switch (ATS16) with Network-MS card Modbus-MS card • Uninterrupted Power Supply (UPSs) with Modbus-MS card	Multiple CVEs	Critical

Overview

Cybersecurity and Infrastructure Security Agency (CISA) has issued an advisory regarding multiple security vulnerabilities affecting Treck Inc.’s TCP/IP stack which is used in some Eaton products to implement IPv4, IPv6, UDP, DNS, DHCP, TCP, ICMPv4 and ARP. These vulnerabilities have been released collectively under the name “Ripple20”. We are currently evaluating the impact of these vulnerabilities to our products, and we are developing mitigation plans to address them.

Vulnerability Details

The effects of the reported Ripple20 vulnerabilities are varied and include classifications such as Improper Handling of Length Parameter Inconsistency, Improper Input Validation, Double Free, Out-of-bounds Read, Integer Overflow or Wraparound, Improper Null Termination, and Improper Access Control.

For more details please refer the below links on individual CVEs –

Eaton Security Bulletin

- 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

Impacted Eaton Product(s) and Version(s)

The following Eaton products directly or indirectly utilize the Treck TCP/IP stack and are therefore impacted by one or more of the reported vulnerabilities:

Control and Relay Products –

- CL-7 voltage regulator control - all firmware versions
- Form 4D recloser control - all firmware versions
- Form 6 recloser control - firmware versions 4.0 and later
- Edison Idea and IdeaPLUS Relays (all variants) - firmware versions 4.0 and later

Power Distribution and Management Products –

- Eaton G3/G3+ ePDU – All firmware versions
  - Metered Input PDU
  - Metered Outlet PDU
  - Managed PDU
  - High Density PDU
- Network Management Card Mini slot (NMC/Network-MS) card – All firmware versions
  - Uninterrupted Power Supply (UPSs) with Network-MS card
  - Automatic Transfer Switch (ATS16) with Network-MS card
- Modbus-MS card – All firmware versions
  - Uninterrupted Power Supply (UPSs) with Modbus-MS card

Note - Eaton will continue to update this list as additional products are evaluated.

Remediation & Mitigation

Remediation

Eaton is currently analyzing the impact of these reported vulnerabilities to our products and preparing appropriate mitigation plans. Eaton recommends that customers follow cybersecurity best practices to further protect their devices, as outlined below. Additional information on remediation and mitigation will be released as it becomes available.

- **Eaton G3/G3+ ePDU** – A new firmware version 4.03.0000 is released to patch the security issues. The new version can be downloaded from here – http://powerquality.eaton.fr/support/software-drivers/downloads/epdu-firmware.asp?cx=80

- **CL-7 voltage regulator control** – Eaton has patched the affected product firmware and released a new version 1.15.2. The latest version can be downloaded from here – https://my.eaton.com/

Interim Mitigation

- 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 business networks.
- 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 VPNs are only as secure as the connected devices.
- Use an internal DNS server that performs DNS-over-HTTPS for lookups.
- Additional mitigation recommendations can be found in ICS Advisory ICSA-20-168-01 and CERT Coordination Center Vulnerability Note VU#257161.

General Security Best Practices

- Restrict exposure to external networks for all control system devices and/or systems and ensure that they are not directly accessible from the open Internet.
- Deploy control system networks and remote devices behind barrier devices (e.g. firewalls, data diodes) and isolate them from business networks.
- Remote access to control system networks should be made available on a strict need-to-use basis. Remote access should use secure methods, such as Virtual Private Networks (VPNs), updated to the most current version available.
- Regularly update/patch software/applications to latest versions available, as applicable.
- Enable audit logs on all devices and applications.
- Disable/deactivate unused communication channels, TCP/UDP ports and services (e.g., SNMP, FTP, BootP, DHCP, etc.) on networked devices.
- Create security zones for devices with common security requirements using barrier devices (e.g. firewalls, data diodes).
- Change default passwords following initial startup. Use complex secure passwords or passphrases.
- Perform regular security assessments and risk analysis of networked control systems.

For more details on cybersecurity best practices and leverage Eaton's Cybersecurity as a Service, please consult the following:

- Eaton offers a suite of cybersecurity assessment and life-cycle management services to help identify vulnerabilities and secure your operational technology network. These services can help you complete the recommended remediation and mitigation actions and strengthen your overall network security. More information about these services are available at www.eaton.com/cybersecurityservices. If you need immediate support, please call +1-800-498-2678 to connect with a representative.
- Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN)
- Cybersecurity Best Practices Checklist Reminder (WP910003EN)

Additional Support and Information

For additional information, including a list of vulnerabilities that have been reported on our products and how to address them, please visit our Cybersecurity web site www.eaton.com/cybersecurity, or contact us at CybersecurityCOE@eaton.com.

Legal Disclaimer:

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. EATON, ITS AFFILIATES, SUBSIDIARIES, AND AUTHORIZED REPRESENTATIVES HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS OF ANY KIND EITHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING, BUT WITHOUT LIMITATION, ANY IMPLIED WARRANTIES AND/OR CONDITIONS OF SECURITY, COMPLETENESS, TIMELINESS, ACCURACY, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS, SO THE ABOVE LIMITATIONS MAY NOT APPLY. TO THE EXTENT PERMITTED BY LAW, IN NO EVENT WILL EATON OR ITS AFFILIATES, OFFICERS, DIRECTORS, AND/OR EMPLOYEES, BE LIABLE FOR ANY LOSS OR DAMAGE OF ANY KIND WHATSOEVER, INCLUDING, BUT NOT LIMITED TO, ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, STATUTORY, PUNITIVE, ACTUAL, LIQUIDATED, EXEMPLARY, CONSEQUENTIAL OR OTHER DAMAGES, EVEN IF EATON HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. EATON RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND AT ITS SOLE DISCRETION.

About Eaton:

Eaton is a power management company. We provide energy-efficient solutions that help our customers effectively manage electrical, hydraulic and mechanical power more efficiently, safely and sustainably. Eaton is dedicated to improving the quality of life and the environment through the use of power management technologies and services. Eaton has approximately 100,000 employees and sells products to customers in more than 175 countries.

Eaton Security Bulletin

Revision Control:

Date	Version	Notes
6/23/2020	v1.0	Initial notification on Ripple20
7/15/2020	V1.1	Updated the list of affected products
7/24/2020	V1.2	Updated the affected product list and updated the mitigation for ePDU products.
8/6/2020	V1.3	Updated the mitigation for CL-7 product.

Office:

Eaton, 1000 Eaton Boulevard

Cleveland, OH 44122, United States

Eaton.com