Eaton Security Bulletin

ETN-SB-2021-1004: Multiple issues in Interniche TCP/IP stack

Publish Date	Impacted Eaton Product(s)	CVE ID(s)	Severity
Dec 2021	• Programmable Logic Controller easyControl EC4P-222… (EC4P)	Multiple CVEs	High

Overview

CISA had released an Industrial Control Systems (ICS) advisory detailing multiple vulnerability in Interniche products in August 2021. An attacker could exploit some of these vulnerabilities to take control of an affected system. The Eaton EC4P-222… products use the Interniche TCP/IP Stack.

Impacted Eaton Product(s) & Version(s)

- Programmable Logic Controller easyControl EC4P… (EC4P)

Vulnerability Details

CVE ID	Description	Affected Component	Potential Impact	CVSSv3.1 Score	Eaton Score
2021-31400	The TCP out-of-band urgent data processing function invokes a panic function if the pointer to the end of the out-of-band urgent data points out of the TCP segment's data, which results in DoS (either an infinite loop or interrupt thrown, depending on NicheStack version).	TCP	DoS	**7.5**	5.2
2021-31401	The TCP header processing code doesn't sanitize the length of the IP length (header + data). With a crafted IP packet an integer overflow would occur whenever the length of the IP data is calculated by subtracting the length of the header from the length of the total IP packet.	TCP	App-dependent	**7.5**	4.6
2020-35683	The code that parses ICMP packets relies on an unchecked value of the IP payload size (extracted from the IP header) to compute the ICMP checksum. When the IP payload size is set to be smaller than the size of the IP header, the ICMP checksum computation function may read out of bounds.	ICMP	DoS	**7.5**	5.2
2020-35684	The code that parses TCP packets relies on an unchecked value of the IP payload size (extracted from the IP header) to compute the length of the TCP payload within the TCP checksum computation function. When the IP payload size is set to be smaller than the size of the IP header, the TCP checksum computation function may read out of bounds. A low-impact write-out-of-bounds is also possible.	TCP	DoS	**7.5**	5.2
2020-35685	TCP ISNs are generated in a predictable manner.	TCP	TCP spoofing	**7.5**	5.2

Remediation & Mitigation

Remediation

Eaton has analyzed the impact of these reported vulnerabilities on the EC4P… products (List of affected products) and is releasing this Security Bulletin for the current and future customers. Eaton recommends that customers follow Hardening/Secure Configuration document to further protect their devices and the mitigation points as outlined below.

Mitigation

The device has an ethernet port which can be used to connect to TCP/IP network. The ethernet port is primarily used to update the firmware or monitor the device operation. The device is susceptible to attack when is it connected to the TCP/IP network. If not connected to network the Interniche stack does not come into picture.

The EC4P… products are approaching EOL and it is not feasible to update the Firmware of these devices. Eaton has performed a risk assessment of the EC4P products for the reported and applicable vulnerabilities.

A Product Lifecycle information document has been published by Eaton for the EC4P… products.

The following mitigation actions should be followed to improve the security of the system.

- Disconnect Ethernet after firmware update or if not using it to monitor the device.
- 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.
- Additional mitigation recommendations can be found in ICS Advisory icsa-21-217-01

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 the 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 the 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 is 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 website 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.

Affected products:

Material Number	Product Name	Description
Y7-106399	EC4P-222-MTXD1	24 VDC,Can,Ethernet,12I,8trans.,displ.
Y7-106400	EC4P-222-MTXX1	24 VDC,Can,Ethernet,12I,8transistor
Y7-106401	EC4P-222-MRXD1	24 VDC,Can,Ethernet,12I,6relay,displ.
Y7-106402	EC4P-222-MRXX1	24 VDC,Can,Ethernet,12I,6relay
Y7-106403	EC4P-222-MTAD1	24 VDC,Can,Eth.,12I,8tr.,displ.,anal.QA
Y7-106404	EC4P-222-MTAX1	24 VDC,Can,Eth.,12I,8trans.,anal.QA
Y7-106405	EC4P-222-MRAD1	24 VDC,Can,Eth.,12I,6rel.,displ.,anal.QA
Y7-106406	EC4P-222-MRAX1	24 VDC,Can,Eth.,12I,6 relay., anal.QA
Y7-106411	EC4P-BOX-222-MTAD	ECP4;XSOFT-CODESYS-2;EU4A-RJ45-USB-CAB1

Revision Control:

Date	Version	Notes
August 2021	1.0	Internal Draft version
December 2021	1.1	added list of affected products.

Office:

Eaton, 1000 Eaton Boulevard

Cleveland, OH 44122, United States

Eaton.com