Eaton Vulnerability Advisory

ETN-VA-2023-1011: easySoft Vulnerability

Date	Overall Risk	CVSS v3.1
19-Oct-2023	Medium	5.9

Overview

Eaton has been made aware of a security vulnerability in the project file of the easySoft software. The easySoft software is used to program easy controllers and displays for configuring, programming and defining parameters for all the intelligent relays and creating visualization functions for the MFD displays.

Vulnerability Details

CVE-2023-43777

CVSS v3.1 Base Score – 5.9 CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L

Eaton easySoft software has a password protection functionality to secure the project file from unauthorized access. This password was being stored insecurely and could be retrieved by skilled adversaries.

Affected Product(s) and Version(s)

Eaton easySoft Software – All versions prior to V8.01

Remediation & Mitigation

Remediation

Eaton has patched the security flaw in the easySoft software version 8.0.1.

Eaton highly recommends that customers and/or end-users migrate to the latest version of easySoft immediately.

Mitigation

Customers are recommended to limit the distribution of project files to trusted entities only and avoid the re-use of passwords.

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.

Eaton Vulnerability Advisory

- 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)

Acknowledgement

Eaton thanks the below researcher(s) for their coordinated support on the security vulnerabilities: -

- CVE-2023-43777 – Manuel Stotz (SySS GmbH)

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 PSIRT@eaton.com.

Legal Disclaimer:

Eaton Vulnerability Advisory

PURPOSE. YOU ARE SOLELY RESPONSIBLE FOR REVIEWING THE USER MANUAL FOR YOUR DEVICES AND GAINING KNOWLEDGE ON CYBERSECURITY MEASURES. YOU SHOULD TAKE THE NECESSARY STEPS TO ENSURE THAT YOUR DEVICE OR SOFTWARE IS PROTECTED, INCLUDING CONTACTING AN EATON PROFESSIONAL. 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 and mechanical power more efficiently, safely, and sustainably. Eaton is dedicated to improving the quality of life and the environment using power management technologies and services. Eaton has approximately 85,000 employees and sells products to customers in more than 175 countries.

Eaton Vulnerability Advisory

Revision Control:

Date	Version	Notes
10/19/2023	v1.0	Initial Vulnerability Advisory

Office:

Eaton, 1000 Eaton Boulevard

Cleveland, OH 44122, United States

Eaton.com