Eaton Vulnerability Advisory

ETN-VA-2020-1009: Multiple security issues in Eaton's easySoft Software

Date	Overall Risk	CVSS v3.0
01/21/2021	Medium	5.8

Overview

Eaton has been made aware of security vulnerabilities in its easySoft software used to program easy controllers and displays. The software provides circuit diagram input and editing, and the diagrams can be displayed in the format desired. An integrated offline simulation tool allows users to test a circuit diagram before commissioning. It supports users who are configuring, programming and defining parameters for all the intelligent relays and creating visualization functions for the MFD displays

Vulnerability Details

CVE-2020-6655

CVSS v3.1 Base Score 5.8 – AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:L

CWE-125: Out-of-bounds read

CWE-20: Improper input Validation

The easySoft software v7.xx prior to v7.22 are susceptible to Out-of-bounds read remote code execution vulnerability. A malicious entity can execute a malicious code or make the application crash by tricking user to upload the malformed .E70 file in the application. The vulnerability arises due to improper validation and parsing of the E70 file content.

References – ZDI-20-1443

CVE-2020-6656

CVSS v3.1 Base Score 5.8 – AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:L

CWE-843: Access to Resource Using Incompatible Type ('Type Confusion')

CWE-20: Improper Input Validation

The easySoft software v7.xx prior to v7.22 are susceptible to file parsing type confusion remote code execution vulnerability. A malicious entity can execute a malicious code or make the application crash by tricking user upload a malformed .E70 file in the application. The vulnerability arises due to improper validation of user data supplied through E70 file which is causing Type Confusion.

References – ZDI-20-1444, ZDI-20-1442, ZDI-20-1441

Note: - There are currently no reports of the vulnerabilities being exploited in the wild.

Affected Product(s) and Version(s)

Product – easySoft Software

Version – 7.xx prior to 7.22

Remediation & Mitigation

Remediation

Eaton has patched the issues and released a new version 7.22. The latest version can be downloaded from Eaton's web site

- easySoft easy Controller and Display Programming Software | Eaton

- Navigate to Eaton software download center -> Select "Software" -> "easySoft" -> v7.22

Mitigation

Only use .E70 files that are either created by you or have been acquired from a fully trusted source.

If the application crashes due to .E70 file upload, restart the application and don't upload the .E70 again.

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)

Acknowledgement

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

- CVE-2020-6655 – Francis Provencher {PRL} working with Trend Micro Zero Day Initiative
- CVE-2020-6656 – Francis Provencher {PRL} working with Trend Micro Zero Day Initiative

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.

Revision Control:

Date	Version	Notes
01/06/2021	v1.0	Initial Notification for the issues.
01/21/2021	V1.1	Added the patch download information.

Office:

Eaton, 1000 Eaton Boulevard

Cleveland, OH 44122, United States

Eaton.com