Hardening documentation

10/2023 MZ048005EN

Product Cybersecurity Guideline easy Remote Touch Display

easy Remote Touch Display Standard
EASY-RTD-DC-43-03B1

easyE Remote Touch Display Advanced
EASY-RTD-DC-43-03B2

EATON

Powering Business Worldwide

Service

For service and support, please contact your local sales organisation.

Contact details: Eaton.com/contacts
Service page: Eaton.com/aftersales

Original Hardening documentation

The English-language edition of this document is the original Hardening documentation.

Translation of the original Hardening documentation

All editions of this document other than those in English language are translations of the original Hardening documentation.

1st Edition 2022, publication date 10/2023

Redaction: Bettina Ewoti

Contents

1 Introduction 2

2 easy Remote Touch Display – Security Instructions......... 3

3 References 7

1 Introduction

easy Remote Touch Display has been designed with cybersecurity in mind. As such, the product offers a number of features for addressing cybersecurity risks. The Cybersecurity Recommendations below have been devised to help users deploy and maintain the product in a manner that minimizes cybersecurity risks. These recommendations are not intended to provide a comprehensive guide to cybersecurity, but rather to complement customers' existing cybersecurity programs.

Eaton is committed to minimizing any cybersecurity risk in its products and to making them more secure, reliable and competitive by deploying cybersecurity best practices.

Several Eaton white papers provide additional information on general cybersecurity best practices and guidelines referenced at

The following whitepapers are available for more information on general cybersecurity best practices and guidelines:

Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):

http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

Cybersecurity Best Practices Checklist Reminder (WP910003EN):
https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/WP910003EN.pdf

2 easy Remote Touch Display – Security Instructions

Category	Description
Intended Use & Deployment Context	The easy Remote Touch Display shall be used to mirror the content of the easyE4's internal display. It shall be enabled to operate the easyE4 with the use of virtual touch buttons. Further, it shall provide a configurable visualization feature to display and set operands of easyE4s. It shall be used in the same context as the easyE4 (applicable for only easyE Remote Touch Display Advanced EASY-RTD-DC-43-03B2). The most typical use case is to mount it in the door of the cabinet, where one or more easyE4s are installed.
Asset Management	Keeping track of software and hardware assets in your environment is a pre-requisite for effectively managing cybersecurity. Eaton recommends that you maintain an asset inventory that uniquely identifies each important component. To facilitate this, easy Remote Touch Display supports the following identifying information: The printing on the enclosure include • manufacturer including location • type ID • serial number • Ethernet MAC-ID • Product QR code (applicable for only easyE Remote Touch Display Advanced EASY-RTD-DC-43-03B2) This information can also be retrieved through these means: • on the device display itself For details see Download Center – Documentation easy Remote Touch Display manual, MN048027.
Risk Assessment	Eaton recommends conducting a risk assessment to identify and assess any foreseeable internal and external risks to the confidentiality, availability and integrity of the system | device and its environment. Any such assessment should be conducted in accordance with the applicable technical and regulatory frameworks. The risk assessment should be repeated periodically.
Physical Security	An attacker with unauthorized physical access can cause serious disruption to system/device functionality. Additionally, Industrial Control Protocols don't offer cryptographic protections, making ICS and SCADA communications especially vulnerable to threats to their confidentiality. Physical security is an important layer of defense in such cases. **easy Remote Touch Display** is designed to be deployed and operated in a physically secure location. Following are some best practices that Eaton recommends to physically secure your system/device: • Secure the facility and equipment rooms or closets with access control mechanisms such as locks, entry card readers, guards, man traps, CCTV, etc. as appropriate. • Restricting physical access to any cabinets and/or enclosures containing **easy Remote Touch Display** and the associated system. Any such access should be monitored and logged at all times. • Restricting physical access to the telecommunication lines and network cabling to protect against any attempts to intercept or sabotage communications. To this end, we recommend using metal conduits for the network cabling between equipment cabinets. • **easy Remote Touch** Display supports the following physical access ports. • Ethernet port • USB port • SD card slot Access to these ports should therefore be restricted. • Only insert SD cards/USB devices with known/valid content for any operation (e.g. Firmware upgrade, Configuration change and Boot application change). • For operations (e.g., firmware upgrades configuration changes or boot application changes) that require the connection of removable media (e.g., USB devices, SD cards, etc.), always make sure that the origin of said media is known and can be trusted. • Before connecting any portable device via a USB port or SD card slot, scan the device for malware and viruses. • Before inserting a SD card/USB device, ensure that no unauthorized **easy Remote Touch Display** firmware is stored on the SD card. • Eaton Cybersecurity Best Practices whitepaper provides additional information about general physical security considerations.

Category	Description
Account Management	Logical access to the system | device should be restricted to legitimate users, who should be assigned only those privileges necessary to complete their roles/functions. Additionally, customers should also consider implementing the following best practices: • Ensuring that default credentials are set upon first login. **easy Remote Touch Display** should not be deployed in production environments with default credentials, as the latter are publicly known. Note: Firmware forces the user to set credentials the first time the device is out into operation. • Account sharing – Each user group is provided with a unique account, and accounts and passwords should only be shared to people with the respective access rights. The product's security monitoring/logging features are designed based on user group accounts. Allowing users to unnecessarily share credentials weakens security. • Restricting administrative privileges – Attackers often seek to gain control of legitimate credentials, especially those used to access highly privileged accounts. Administrative privileges should thus only be assigned to people that are designated for administrative duties and not intend to use the device regularly. • Leveraging the roles / access privileges to grant users tiered access in line with business /operational needs, following the principle of least privilege (by allocating users only that level of authority and access to system resources that is required to perform their role). • Ensuring that complexity is appropriately set, particularly for the administrative account and that the passwords are changed after expiry every 90 days or as otherwise stipulated by the customer's policies.
Time Synchronization	Easy Remote Touch Display only uses its system time for log files. Ensure time synchronization provided in the device are properly configured. The device offers different options to synchronize system time: NTP and automatically retrieving date/time when connecting to an easyE4 (since FW version v1.1.0.0 for EASY-RTD-DC-43-03B1 and version v1.0.0.0 for EASY-RTD-DC-43-03B2). (for instructions see manual)
Network Security	**easy Remote Touch Display** supports network communication with other devices in its environment. This capability may present certain risks if not configured securely. Eaton recommends the following best practices to help secure the network. Additional information about various network protection strategies is available in the Eaton white paper Cybersecurity Considerations for Electrical Distribution Systems [R1]. Eaton recommends segmenting networks into logical enclaves, denying any traffic between segments except that which is specifically allowed, and restricting any communication to host-to-host paths (for example, by using router ACLs and firewall rules). This helps to protect sensitive information and critical services and creates additional barriers in the event of a network perimeter breach. At a minimum, a utility Industrial Control Systems network should be segmented into a three-tiered architecture (as recommended by NIST SP 800-82[R3]) for better security control. Deploy adequate network protection devices like Firewalls, Intrusion Detection / Protection devices. Please find detailed information about various Network level protection strategies in Eaton Cybersecurity Considerations for Electrical Distribution Systems [R1]. Use the below information for configuring the firewalls to allow needed access for **easy Remote Touch Display** to operate smoothly. UDP port 11111: Discovery service for device identification. The device delivers information about itself on request. UDP port 11112: Used to communicate with easyE4 devices. The UDP communication is protected by a cryptographic hash. The device should only be operated in a secure network environment. TCP port 11119: TLS protected service to open a display session and/or visualization communication in easyE4 for **easy Remote Touch Display**. UDP port 11113: Used to communicate with easyE4 devices. The UDP communication is protected by a cryptographic hash. The device should only be operated in a secure network environment. Note: Many compliance frameworks and cybersecurity best practices require an audit of ports and services before and after applying updates and system changes. An end user should be able to refer to the ports and services documentation to determine the expected minimal set of ports and services on a device Websockets port 80: protocol to communicate with easySoft: download/upload of device configuration and visualization projects, get device information, set RUN/STOP state of device. For details, see the easyE RTD manual. The access is protected using the device's admin user group password.

Category	Description
Logging and Event Management	- Eaton recommends logging all relevant system and application events, including all administrative and maintenance activities. - The logs should be protected from tampering and other risks to their integrity (for example, by restricting the permissions to access and modify them, by transmitting them to a security-information and event-management system, etc.). - The logs should always be retained for a reasonable and appropriate length of time. - The logs should be regularly reviewed. A reasonable review frequency should be selected, taking into account the sensitivity and criticality of the system | device and any data it processes. - The **easy Remote Touch Display** itself automatically logs events such as operating system log, login/logout, easyE4 connections, configuration changes and security related inconsistencies in the communication (hash faults). - Logs are automatically done and can be exported in the log section of the device information page using an external storage device (SD card or USB stick). This includes: Logon, logoff, linux boot sequence, external storage device attachment/detachment, security hash faults, system errors and firmware updates. - Only Admin user group has the rights to view or export logs.
Malware Defenses	Eaton recommends deploying adequate malware defenses to protect the product as well as the platforms used to run it.
Secure Maintenance	The device includes a possibility to copy log files to a USB stick to SD card. This can only be done by using the Admin account or by Eaton personnel using the Service account. The Service account is not visible to and not to be used by to the customer by default. It shall be used for troubleshooting and diagnostic purposes. **Best Practices** The device firmware should be updated prior to putting the device into production. Thereafter, firmware updates and software patches should be applied regularly. Eaton regularly publishes patches and updates for its products to protect them against any vulnerabilities that are discovered. Eaton encourages customers to consistently monitor the availability of new firmware updates and to install them promptly. - A firmware update file can be downloaded from the Eaton website. This file has to be placed on an SD card or USB stick. After the device has been attached to the **easy Remote Touch Display** the user can choose the update tab in the device menu and update the firmware. Please check Eaton's website for information bulletins about available firmware and software updates Download Center – Software. Please visit the product website easyE4 programmable relay visualization (eaton.com)
Business Continuity / Cybersecurity Disaster Recovery	**Plan for Business Continuity / Cybersecurity Disaster Recovery** It's a Cybersecurity best practice for organizations to plan for Business continuity. Establish an OT Business Continuity plan, periodically review and, where possible, exercise the established continuity plans. Make sure offsite backups include Backup of the latest f/w copy of **easy Remote Touch Display**. Make it a part of SOP to update the backup copy as soon as the latest f/w is updated. Documentation of the most current User List. Following section describes the details of failures states and backup functions If a firmware update fails, the display will show an error message with the specific cause of the failure. Solution: in case of a firmware signature failure, please check if you have downloaded a valid version from the EATON website: Download Center – Software. Other failures may occur due to file corruptions. Please download the firmware again and use a FAT/FAT32 formatted device to install the firmware on the **easy Remote Touch Display**. If the communication is interrupted or spoofed the user gets a message on the screen about the specific failure. For further details see device manual.
Sensitive Information Disclosure	A Eaton recommends that any sensitive information (i.e., information about connectivity, log data or personal information) that may be stored by **easy Remote Touch Display** be adequately protected through the deployment of organizational security practices.

<table>
<tr><th>Category</th><th>Description</th></tr>
<tr><td>Decommissioning or Zeroisation</td><td>

It is a best practice to purge data before disposing of any device containing data. Guidelines for decommissioning are provided in NIST SP 800-88. Eaton recommends that products containing embedded flash memory be securely destroyed to ensure that the data are unrecoverable.

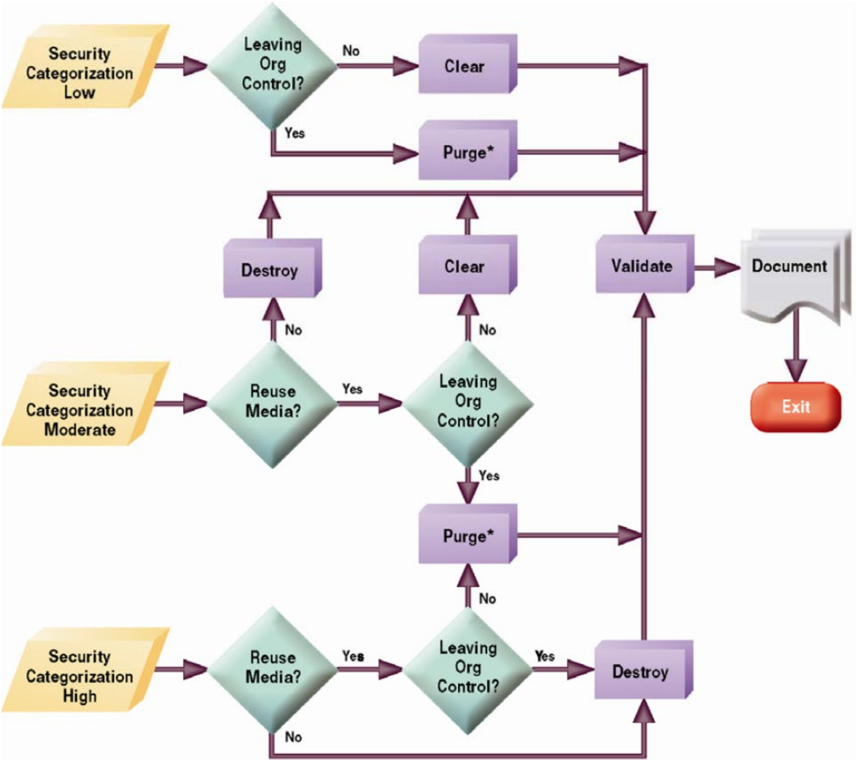

Figure 4-1: Sanitization and Disposition Decision Flow; Source: NIST SP800-88

Embedded Flash Memory on Boards and Devices

- Eaton recommends the following methods for disposing of motherboards, peripheral cards such as network adapters, or any other adapter containing non-volatile flash memory.
- **Clear**: Where possible, the device should be reset to the original factory settings
  The **easy Remote Touch Display** supports a factory reset through a Button in the device info tab when logged in as Admin. Factory reset is also possible through powering up the device and once the display lit hold the CTRL button ont the left side of the device enclosure for at least 5 seconds and relesease it.
- **Purge**: If the flash memory can be easily identified and removed from the board, it may be destroyed independently of the board that contained it. Otherwise, the whole board should be destroyed.
  The SD card and /or USB stick of easy Remote Touch Display can be removed from the device and destroyed separately. The internal flash memory should be destroyed as part of the whole board
- **Destroy**: The device should be shred, disintegrated, pulverized or incinerated by burning it in a licensed incinerator.

</td></tr>
</table>

3 References

[R1] Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):
http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

[R2] Cybersecurity Best Practices Checklist Reminder (WP910003EN):
http://www.cooperindustries.com/content/dam/public/powersystems/resources/library/1100_EAS/WP910003EN.pdf

[R3] NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015:
https://ics-cert.us-cert.gov/Standards-and-References

[R4] National Institute of Technology (NIST) Interagency "Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41", October 2009:
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

[R5] NIST SP 800-88, Guidelines for Media Sanitization, September 2006:
http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819

[R6] Cybersecurity Best Practices for Modern Vehicles - NHTSA

https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

[R7] A Summary of Cybersecurity Best Practices - Homeland Security

https://www.hsdl.org/?view&did=806518

Eaton is dedicated to ensuring that reliable, efficient and safe power supply is available when it is needed most. With vast of energy management across different industries, experts at Eaton deliver customized, integrated solutions to solve our customer' most critical challenges.

Our focus is on delivering the right solution for the Application. But decision makers demand more than just Innovative products. They turn to Eaton for an unwavering Commitment to personal support that makes customer Success a top priority.
For more information, visit **Eaton.com**

Eaton addresses worldwide:
Eaton.com/contacts

EATON
Powering Business Worldwide

Eaton Industries GmbH
Hein-Moeller-Str. 7- 11
D-53115 Bonn

10/2023 MZ048005EN