Eaton Vulnerability Advisory

ETN-VA-2024-1026: Vulnerabilities reported in i-WiFi01

Date	Overall Risk	CVSS v3.0
11/08/2024	Critical	10.0

Overview

Eaton has been notified about multiple vulnerabilities affecting Eaton's IP intruder system adaptor i-WiFi01. The adaptor is used to provide wireless capabilities to Eaton's alarm panels including i-on and COMPACT panels. As cybersecurity standards continue to evolve and to meet our requirements today, we have decided to End-of-Life the product. Upon retirement or end of support, there will be no new security updates, non-security updates, or paid assisted support options, or online technical content updates.

Vulnerability Details

- Unauthenticated RCE via stack-based buffer overflow (CVE-2024-39791)
- Hardcoded credentials (CVE-2024-41161)
- Unauthenticated factory reset (CVE-2024-29082)
- Unauthenticated directory traversal (CVE-2024-41936)
- Authenticated command injection (CVE-2024-37023)
- Unauthenticated DoS (CVE-2024-39815)
- Unauthenticated direct request (CVE-2024-42001)

Affected Product(s) and Version(s)

- Eaton i-WIFI01

Remediation & Mitigation

Remediation

Eaton has decided to end-of-life the IP intruder system adaptor i-WiFi01 effective 2nd October 2024. (End-of-life notification - Link)

The customers are advised to upgrade to COM-DATA-WIFI as soon as possible, which is a fit and functional replacement for the i-WiFi01 adaptor.

In the case of the COMPACT panel, we recommend customers to consider alternative 3rd party Wi-Fi network connectivity modules or use mobile connectivity via the COM-DATA-4G-SD.

Eaton Vulnerability Advisory

Mitigation

Eaton recommends implementing the below mitigation measures in case the users are unable to migrate to the above replacement options.

- Disable local and network access to the panel web server.
- Ensure that the Wi-Fi adaptor is configured to a secure Wi-Fi network. Do not leave the Wi-Fi adaptor unconfigured.
- Change the default credentials of the Wi-Fi module and Wi-Fi access point to a complex or a unique alpha-numeric password with special characters.
- Only permit trusted devices to connect to the Wi-Fi network. Leverage IP/MAC whitelisting functionality. (If supported)
- Ensure that the software of the Wi-Fi router is updated to the latest version.
- Ensure firewall functionality is enabled on the router to prevent malicious traffic.
- When remote access is required to the panel, 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.

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 PSIRT@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. 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
11/08/2024	v1.0	Initial notification

Office:

Eaton, 1000 Eaton Boulevard

Cleveland, OH 44122, United States

Eaton.com