Date:	February 28, 2017
Subject:	Advisory on Eaton xComfort
Severity rating:	Medium
Product:	xComfort Ethernet Communication Interface (ECI)
Affected version:	All firmware versions V01.07 and below

Summary

ICS-CERT recently contacted Eaton regarding potential vulnerability with earlier versions of our xComfort Ethernet Communication Interface cards. These products were designed to be used with Eaton's xComfort system to connect xComfort devices in larger buildings over Ethernet infrastructure.

Impact on products

The following Eaton products have been identified as having the impacted firmware.

Information	Part number
Ethernet Communication Interface (ECI)	**CCIA-02/01**
Ethernet Communication Interface (ECI) POE	**CCIA-03/01**

Additional information regarding these and other legacy products can be found on the link below.

http://www.eaton.eu/Europe/Electrical/ProductsServices/Residential/xComfort-RFSmartHomeSolutions/index.htm?wtredirect=www.eaton.eu/xcomfort#tabs-11

Vulnerability overview

An attacker could potentially access (read) backup file and system logs without being authenticated. If sensitive information is present in the logs (e.g.: plaintext credentials), the malicious user can then use it to further compromise the system.

There is no known evidence that this vulnerability has been exploited in a production environment.

Exploitability and severity rating

An attacker exploits these vulnerabilities using an authentication bypass.

The U.S. Department of Homeland Security has adopted the Common Vulnerability Scoring System (CVSS) that provides an open framework for communicating the characteristics and impact to system vulnerabilities, how difficult they are to exploit, and the impact on a successful attack based on the exploit of the vulnerability.

In a typical recommended deployment of these products as outlined in the section below, our assessment is that this vulnerability rates as low. However, failure to institute the standard recommended security procedures, or exploitation by an internal individual or others behind a user's firewall, would result in a high vulnerability to this type of attack.

Recommended course of action

Eaton recommends that users download firmware v1.08 plus v2.10 and apply to their affected products.

References

ICS-VU-513757

Additional information

For additional information or 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.

Powering Business Worldwide

Follow us on social media to get the latest product and support information.

Eaton is a registered trademark.

All other trademarks are property of their respective owners.