ePDU vulnerability
ICS-VU-148812 communications—external website

Date: November 15, 2016	
Subject: Advisory on Eaton G2 ePDU	
Severity rating: Medium	
Product: Advanced Monitored ePDUs G2	
Affected version: All versions V01.01.0011 and below	

Summary

ICS-CERT recently contacted Eaton regarding potential vulnerability with earlier versions of our Advanced Monitored ePDUs (G2). These products were designed to provide manageability, control and power consumption monitoring at the outlet level for servers.

Vulnerability overview

An attacker could potentially exploit this vulnerability by gaining administrative privileges without being authenticated.

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

Impact on products

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

Product	Date
ePDU G2 Catalog	Date Discontinued (End of Life)
EAMxxx	June 30, 2015
EMAxxx	January 31, 2014
EAMAxx	
EMAAxx	
ESWAxx	

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

http://powerquality.eaton.com/EMEA/Products-services/Legacy/Legacy-Products.asp

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 "Recommended course of action", 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

The above products were end-of-life (EoL) by Eaton on January 31, 2014 and June 30, 2015, as shown in "Impact on products" of this advisory. Eaton recommends that users of the affected legacy products follow the recommendations outlined in Eaton's "Cybersecurity considerations for electrical distribution systems" whitepaper under the section "Defense in depth".

For more information:

Pre-sales support
800.356.5794
InsideSalesEngineerUPS@eaton.com

References

ICS-VU-148812

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

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

Printed in USA
Publication No. SB152031EN / Z18966
November 2016

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