

glibc vulnerability (CVE-2015-0235): GHOST

Electrical Sector's Product Cybersecurity team recommendations for glibc vulnerability

Summary

Eaton is aware of and has released a solution for a vulnerability found in Linux systems involving the glibc library that was assigned CVE-2015-0235. This vulnerability is also referred to as GHOST.

Vulnerability overview

GHOST is a 'buffer overflow' bug affecting function calls in the glibc library that could potentially allow someone to execute remote code. The vulnerability is reported against glibc libraries versions 2.2 to 2.17.

Impact on products

The following Eaton products have been identified as utilizing the impacted glibc libraries.

Power Xpert® Gateway models:

- PXG 200E
- PXG 400E
- PXG 600E
- PXG 800E
- PXM 2000
- PXMP
- PXM 4000/6000/8000

Exploitability and severity rating

The glibc libraries versions 2.2 to 2.17 are vulnerable to buffer overflow and potential remote code execution.

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. The CVSS for this vulnerability is high.

Recommended course of action

Eaton recommends that users of the affected products follow the recommendations outlined in Eaton's "Cybersecurity considerations for electrical distribution systems" whitepaper under the section "Defense in depth" at the link below. http://www.eaton.com/ecm/idcplg?IdcService=GET_FILE&all_owlInterrupt=1&RevisionSelectionMethod=LatestReleased&noSaveAs=0&Rendition=Primary&dDocName=WP152002EN

Eaton has fixed the issue in the latest firmware releases for these products as follows:

- Power Xpert Gateway 200E/400E/600E/800E version released v.3.0.8 or above
- PXM 2000 firmware v.2.1.4
- PXMP 2.0 with Energy Portal firmware v.2.3
- PXM 4000/6000/8000 firmware v.13.3.5.6

References

- <https://access.redhat.com/security/cve/CVE-2015-0235>
- http://www.cvedetails.com/vulnerability-list/vendor_id-72/product_id-767/GNU-Glibc.html

For additional information or for a list of other issues potentially affecting our products and how to address them, please visit our Cybersecurity website at Eaton.com/cybersecurity or email CybersecurityCOE@eaton.com.

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

© 2015 Eaton
All Rights Reserved
Printed in USA
Publication No. SA152007EN / Z16819
June 2015

Eaton is a registered trademark.

All other trademarks are property of their respective owners.