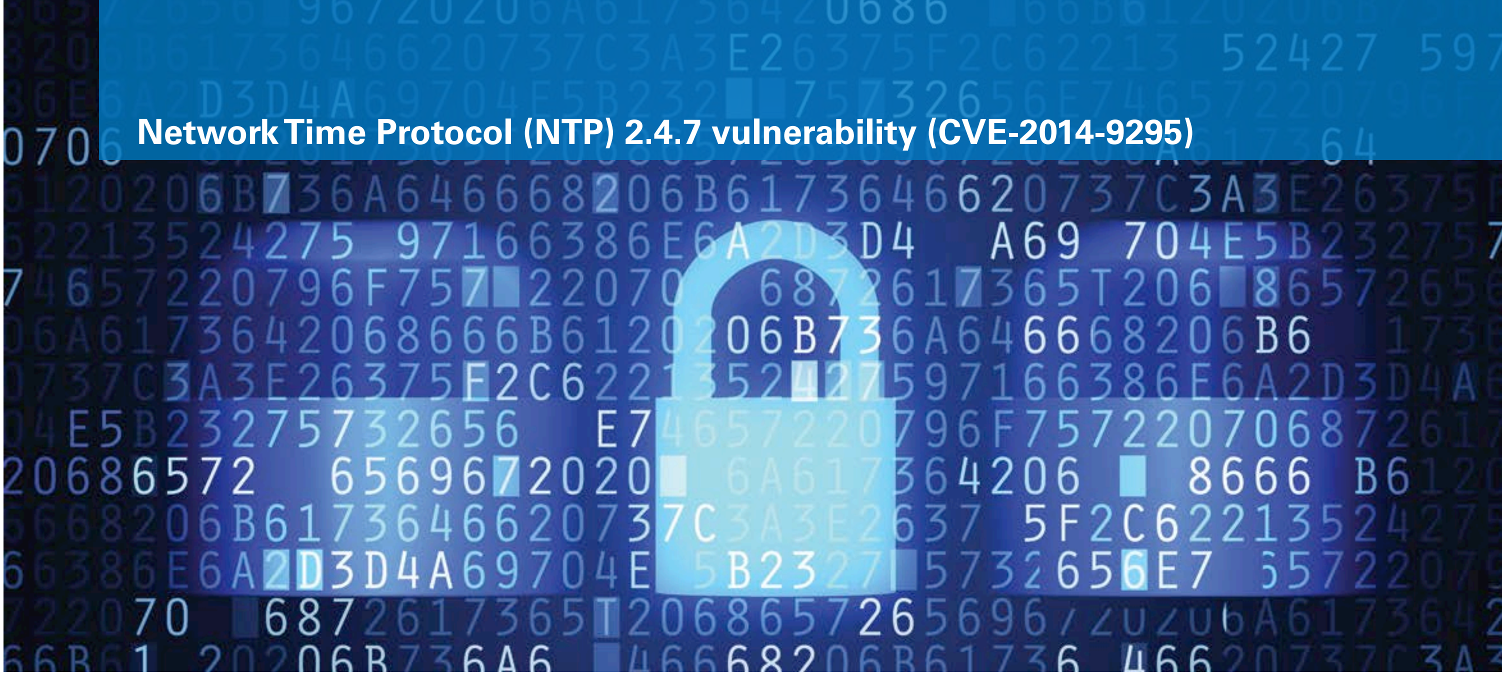

## Network Time Protocol (NTP) 2.4.7 vulnerability (CVE-2014-9295)

# Electrical Sector's Product Cybersecurity team recommendations for NTP vulnerability

### Summary

US-CERT has issued an alert about vulnerability in the Network Time Protocol (NTP) (CVE-2014-9295) that can be exploited by someone executing arbitrary code with the privileges of the ntpd process.

The Network Time Protocol (NTP) provides networked systems and devices with a way to synchronize time for various services and applications.

### Vulnerability overview

The vulnerability is reported against Network Time Protocol (NTP) code library versions 4.2.7 and below and can be exploited by allowing a buffer overflow or potential remote code execution.

### Impact on products

The following Eaton products have been identified as utilizing the NTP library.

Power Xpert® Gateway models:

- PXG 200E
- PXG 400E
- PXG 600E
- PXG 800E

### Exploitability and severity rating

The Network Time Protocol (NTP) versions 4.2.7 and below 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 and 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&allowInterrupt=1&RevisionSelectionMethod=LatestReleased&noSaveAs=0&Rendition=Primary&dDocName=WP152002EN

Eaton has fixed the issue in the latest firmware release, v.3.0.8 of the Power Xpert Gateway 200E/400E/600E/800E. Please contact the Customer Success Team at 1-800-809-2772, option 4, or 414-449-7100, option 4, or email pqsupport@eaton.com to address any questions or obtain the latest firmware version release.

### References

- Network Time Protocol Vulnerabilities (Update A) https://ics-cert.us-cert.gov/advisories/ICSA-14-353-01A
- http://www.kb.cert.org/vuls/id/852879
- http://www.ntp.org/downloads.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

Printed in USA
Publication No. SA152009EN / Z16246
February 2015

EATON
*Powering Business Worldwide*

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