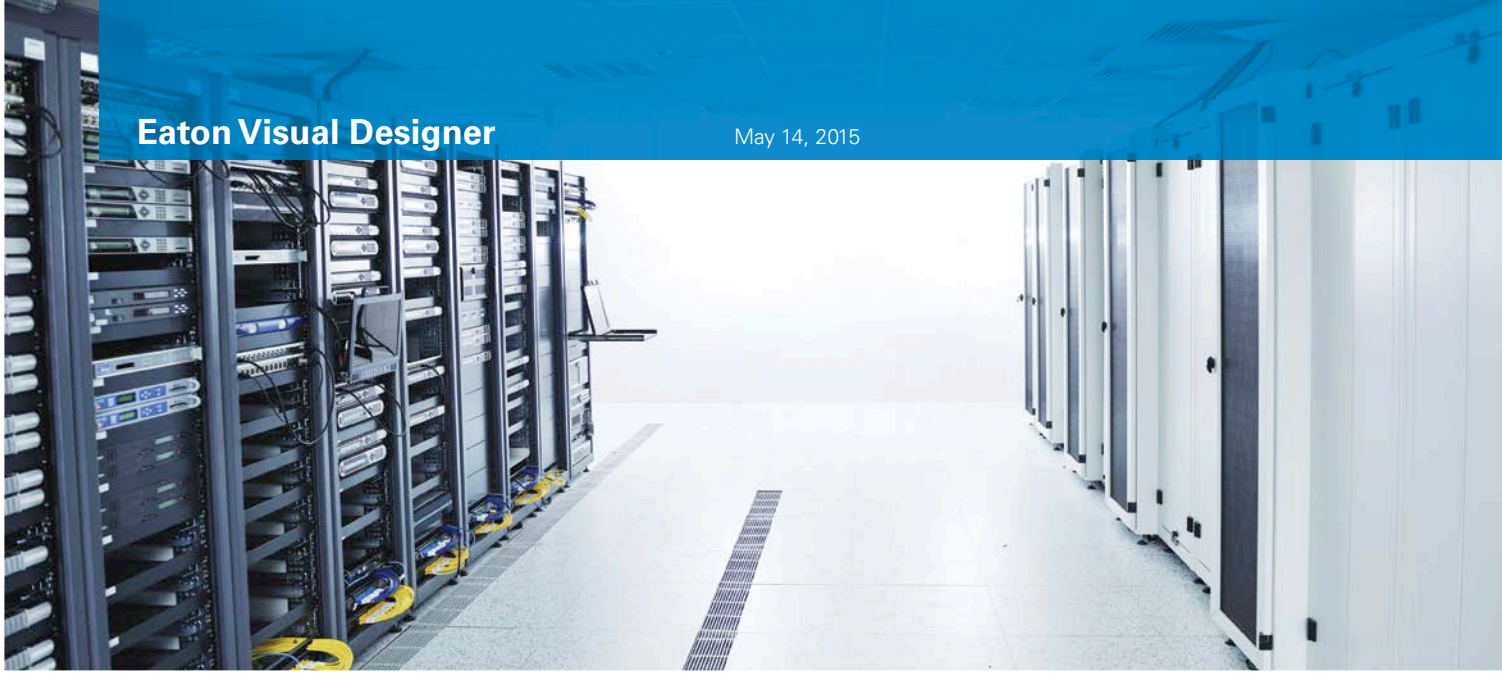

Advisory on Eaton's Visual Designer

All versions from V7.0.0.0 through V7.1.3.3

Summary

Eaton has become aware of and has released a fix for a vulnerability involving Eaton's Visual Designer software.

Vulnerability overview

An attacker who exploits these vulnerabilities may be able to execute arbitrary code.

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

Impact on products

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

- Eaton's XP-702 and XP-503 Panel PC/Operator Interface
  - XP-702-E0-84TSIJ-10
  - XP-702-E0-10TSIJ-10
  - XP-702-E0-12TXIJ-10
  - XP-702-E0-15TXIJ-10
  - XP-702-E0-BOXJ-00
  - XP-702-F0-84TSIK-10
  - XP-702-F0-10TSIK-10
  - XP-702-F0-12TXIK-10
  - XP-702-F0-15TXIK-10
  - XP-702-F0-BOXK-00
  - XP-503-10-A10-A00-1V
  - XP-503-15-A10-A00-1V
  - XP-503-21-A10-A00-1V
- Eaton's Visual Designer PC runtime software
  - VISUALRTPC300
  - VISUALRTPC1500
  - VISUALRTPC4K
  - VISUALRTPC64K

Exploitability and severity rating

An attacker who exploits these vulnerabilities may be able to execute arbitrary code.

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.

Our assessment of this vulnerability rates this security update as **medium**.

Recommended course of action

Eaton has released new patches that mitigate this vulnerability at the link below. Eaton recommends all our customers using the products above to upgrade to these latest versions.

Visual Designer 7.1 Service Pack 3, Patch 5

References

http://ics-cert.us-cert.gov/advisories/ICSA-15-085-01A

Other information

Cybersecurity standards and best practices

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 here.

For additional information or for a list of vulnerabilities that have been reported on our products and how to address them, please visit our Cybersecurity website **Eaton.com/cybersecurity** contact us at **CybersecurityCOE@eaton.com**.

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

Printed in USA
Publication No. MZ152007EN / Z16694
May 2015

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

Powering Business Worldwide