Date:	**February 15, 2018**
Subject:	**ELCSoft Programming Software**
Severity rating:	Medium
Product:	All versions of ELCSoft programming software
Affected version:	All versions V2.04.02 and below

1. Summary

ICS-CERT recently contacted Eaton regarding potential vulnerabilities with our ELCSoft programming software. ELCSoft programming software is used to configure all Eaton ELC programmable logic controllers deployed in many industrial sectors including power distribution applications deployed by power grid operators to apply protection and communications support for overcurrent devices such as reclosers and circuit breakers. This product is used widely in the Energy Sector on a worldwide basis. While the ELC controllers themselves do not exhibit this vulnerability, the Microsoft Windows(r) based PCs used to configure the logic in the ELC exhibit this vulnerability when running the ELCSoft editor.

2. Recommended Course of Action

Eaton has released a new revision that eliminates these vulnerabilities. Eaton recommends all our customers using the products above to uninstall the prior version before installing the new software.

ELCSoft Version 2.7

3. References

ICS-ALERT-17-216-01, ICSA-16-182-01

4. 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" on the link here.

Support

For additional information or a list of vulnerabilities that have been reported on our products and how to address them please visit our Cybersecurity web site www.eaton.com/cybersecurity or you can contact us at CybersecurityCOE@eaton.com.