TCP/IP protocol non-conformances and potential vulnerabilities affecting Eaton's Cooper Power series Form 6 recloser control and Idea/IdeaPLUS relay

Severity rating:
Low

Product(s):
Form 6 control and Idea/IdeaPLUS relays with Ethernet

Affected versions:
All versions of Eaton's Cooper Power series Form 6 control and Idea/IdeaPLUS relays with Ethernet, with ProView™ 4.0 through ProView 5.0 software

Summary

ICS-CERT recently contacted Eaton regarding potential vulnerabilities with the TCP/IP protocol stack utilized by the Cooper Power™ series Form 6 recloser control and Idea™/IdeaPLUS™ relay protection platforms. These products are deployed in large numbers by power grid operators to apply protection and communications support for overcurrent devices such as reclosers and circuit breakers. Many are currently not actively connected to a communications network; but, those that are communicating are typically connected to private communications systems.

In this bulletin, we describe the reported TCP/IP protocol stack vulnerabilities that affect the Form 6 control and Idea/IdeaPLUS relay, their applicability to the network, and the methods that users should have in place to enhance secure operation of their systems.

Reported TCP/IP protocol stack vulnerabilities

Academic researchers identified, and Eaton has confirmed, potential issues in the networking implementations in the above named products. These issues were reported as vulnerabilities that arise out of non-conformance with network standards. These could allow for the potential of spoofing attacks, session hijacking, or re-transmission of old data as frame padding.

Applicability to the network

The effects of exploiting the reported sequence number predictability non-conformance are the same as the effects of an attacker connecting directly to the control or network and listening for or initiating a new session. Although an issue exists, it must be noted that no authentication mechanism is used for new socket connections to SCADA protocol (e.g., DNP3) listening ports on the Form 6 control and Idea/IdeaPLUS relays. Thus, the importance of deploying network segmentation and isolation on the control system network is further underscored. By ensuring that controls are not accessible from external networks and that appropriate physical security measures are provided at network access points, any risks associated with this vulnerability are greatly minimized.

The effects of exploiting the Ethernet frame padding non-conformance are limited to viewing the previously transmitted data that has been used to pad undersized Ethernet frames. No further exploitability is expected, any risk is further minimized by implementing appropriate network and physical security measures, and the identified issues are eliminated by implementing the newer versions of software/firmware described below.

Eaton's Cooper Power Systems division has developed ProView 5.1 software and firmware that mitigates these non-conformances in the Form 6 recloser control. ProView 5.1 for the Form 6 control was released on August 6, 2015. Additionally, ProView 5.0 Revision 11 software and firmware has been developed to mitigate these issues in the Idea/IdeaPLUS relay. ProView 5.0 Revision 11 upgrades for the Idea/IdeaPLUS relay were posted starting on June 30, 2015. ProView 5.0 revision 11 and ProView 5.1 are compatible with any hardware and firmware versions 5.0 and higher (expanded memory hardware). Versions below 5.0 (non-expanded memory hardware) may be updated with the appropriate and corresponding hardware upgrades. Information on how to obtain and install these available remedies are available through the following links:

Link to Form 6 reclosure control remedies

Link to Idea/IdeaPLUS relay remedies

Powering Business Worldwide

TCP/IP protocol non-conformances and potential vulnerabilities affecting Eaton's Cooper Power series Form 6 recloser control and Idea/IdeaPLUS relay

Recommended course of action

Eaton recommends that customers using these products take advantage of the most recent software/firmware versions available, and take steps to ensure that they exercise system-wide defensive in-depth strategies as outlined in our whitepaper Cybersecurity considerations for electrical distribution systems.

References

NCCIC/ICS-CERT Advisory ICSA-15-006-01

NCCIC/ICS-CERT Advisory ICSA-15-279-01

Customer support contact information

Contact our Eaton Electrical Sector Cybersecurity team at CybersecurityCOE@eaton.com or our technical support team at res-pssm-ssg@eaton.com or 1.800.497.5953.

Customer support is available on weekdays between 7 a.m. and 4 p.m. Eastern Standard Time.

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

Printed in USA
Publication No. SA152018EN / Z17420
October 2015

Powering Business Worldwide