Security Notification – MiCOM Px30 and Px40 Digital Protection Relays

29-Feb-2016

Overview

Schneider Electric was notified and is responding to vulnerability in the MiCOM Px30 Series and MiCOM Px40 Series digital protection relays.

Vulnerability Overview

The vulnerability identified is related to the RPC (remote procedure call) component of VxWorks operating system enabling a maliciously-crafted packet to cause an integer overflow, with the possibility of executing remote code.

Product(s) Affected

The product affected:

- MiCOM Px30 Series all versions
- MiCOM Px40 Series all versions

Vulnerability Details

An Integer overflow attack through RPC (port 111) might lead to Remote Code execution. If successfully exploited, this vulnerability leads to lack of **availability** of communication features. This potential operation can result in forbidding Ethernet connection from MiCOM S1 Studio to the attacked relay. The serial connection remains unaffected. Temporary loss of communication functionalities can occur, including IEC61850 protocol (Goose and MMS) or DNP3oE. Only firmware of network boards is affected.

The core protection functionalities aren't affected. The protection functions remain fully operational.

Overall CVSS Score: 4.3

[AV:N/AC:M/Au:N/C:N/I:N/A:P]

Mitigation

Schneider Electric is working to resolve the issue raised in this document.

In next release of MiCOM Px30 Series and MiCOM Px40 Series digital protection relays, RPC component of VxWorks OS will be removed and replaced by a strong TLS based component. So the vulnerability will be removed. In the meantime, the following General Recommendations should be heeded to protect the installation.

General Recommendations

Schneider Electric has been designing industrial automation products for many years; Schneider Electric follows, and recommends to its customers, industry best practices in the development and implementation of control systems. This recommendation includes a Defense in Depth approach to secure an Industrial Control System.

Download our cybersecurity whitepaper from https://www.Schneider-electric.com. See Support > Cybersecurity

Mitigation actions can be taken in order to reduce risk.

- Secure Network access (Switch Configuration, Physical Security).
- Put in place Network Intrusion Detection System.

For Secure Network Access is recommended to define strong hardening rules in Network Devices:

- Disable Unused Services and port (Secure management protocol, Physical port, VLAN)
- Least privilege
- Central Account management
- IP filtering
- MAC Change notification
- Log Management (Audit)

For Network Intrusion Detection mitigation, it is recommended to use an advanced firewall in the architecture in order to detect intrusion on the network. Intrusion Detection System rules have to be defined following environment's constraints.

Put special attention in the protection of TCP and UDP 111 and 1006.

For More Information

This document is intended to help provide an overview of the identified vulnerability and actions required to mitigate it. To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric representative. These organizations will be fully aware of the situation and can support you through the process.

For further information on vulnerabilities in Schneider Electric's products, please visit Schneider Electric's cybersecurity web page at http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

About Schneider Electric

As a global specialist in energy management with operations in more than 100 countries, Schneider Electric offers integrated solutions across multiple market segments, including leadership positions in Utilities & Infrastructures, Industries & Machine Manufacturers, Non-residential Buildings, Data Centers & Networks and in Residential.
www.schneider-electric.com

Product Security Office

Digitally signed by Product Security Office
DN: cn=Product Security Office, o=Schneider Electric, ou=Global Technology, email=cybersecurity@schneider-electric.com, c=US
Date: 2016.03.02 08:16:51 -05'00'