SAGE 3030 RTU DNP3 Input Validation Vulnerability

December 30, 2013

Overview

Schneider Electric has become aware of a vulnerability in the Schneider Electric SAGE 3030 product line which could result in remote exploitation resulting in Denial of Service. A software patch has been released remediating this vulnerability.

Vulnerability Overview

The vulnerability identified includes improper DNP3 input validation which could result in successful denial of service attack on the SAGE 3030 products specified in this document.

Product(s) Affected

The products affected are:

- SAGE 3030 C3413-500-001D3_P4
- SAGE 3030 C3413-500-001F0_PB

Vulnerability Details

Successful exploitation of this vulnerability could allow an attacker to affect the availability of the DNP3 master-slave communication in Telvent SAGE 3030 and similar devices. CVSS Base Score = 5.4.

Report Confidence

The exploit proof of concept has been confirmed.

Exploitability Metrics

Access Vector – Network

- The attacker requires network access to the SAGE 3030.

Access Complexity – High

- The attacker must acquire physical or virtual access to a network on which the SAGE 3030 resides.

Authentication – None

- A successful attack does not require authentication.

Impact Metrics

Confidentiality Impact– None. A successful attack will not impact the confidentiality of the RTU system.
Integrity Impact – None. A successful attack will not impact the integrity of the RTU system.
Availability Impact– Complete. A successful attack will cause shutdown of the affected resource.

Exploitability – A successful attack has been proven, no known exploits have been published.

Remediation Level – An official vulnerability fix exists. Details for accessing this fix are contained in this document.

Source:
http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:H/Au:N/C:N/I:N/A:C/E:P/RL:O/RC:C)#score

Mitigation

Schneider Electric has created a patch to mitigate this vulnerability on the C3414 LX-800 based RTUs using latest VX-works 6.9.3 OS. Customers may obtain this patch by contacting Schneider Electric Customer Service Department at 713-920-6832.

Product:
C3414-500-S02YZ - Secure Firmware version J0

In addition to better checking of DNP3 input for malformed packets, the J0 firmware includes features for encryption, authentication, improved logging, and DNP3 connection port validation:

- **HTTPS – secure browser**
- **SSH – secure Telnet connectivity**
- **SFTP – secure file transfer**
- **SSL – secure Ethernet**
- **Firewall/IPsec – secure networks**
- **Secure User Management**

Reference:
NCCIC/ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cyber security risks.

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

This document is intended to help provide an overview of the identified vulnerability and recommended remediation actions. To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric Customer Service or Support representative.

For further information on vulnerabilities in Schneider Electric's products, please visit Schneider Electric's Cybersecurity Site 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