Security Notification – SAGE RTU

12-Mar-2016

Overview

Schneider Electric has become aware of a vulnerability in the SAGE RTU's related to improper Ethernet frame padding.

Vulnerability Overview

The data padding within the data field of the Ethernet pack should be all zeros. The firmware allowed other data from a known area of memory to be used in this field and could exfiltrate or leak data.

Product(s) Affected

The products affected:

C3414 CPU based SAGE RTU's:

- SAGE 3030M, with firmware prior to C3414-500-S02J2 (released March 2015.)
- SAGE 1410, 1430, 1450 with firmware prior to C3414-500-S02J2.
- LANDAC II, with firmware prior to C3414-500-S02J2.
- SAGE 2400, with firmware prior to C3414-500-S02J2.

C3413 CPU based SAGE RTU's

- SAGE 2300, 1310, 1330, 1350, 3030 with all firmware versions.
- LANDAC with all firmware versions.

Vulnerability Details

IEEE 802 specifies that packets have a minimum size of 56 bytes. The Ethernet driver is expected to fill the data field with octets of zero for padding when packets are less than 56 bytes. Resident memory and other data are used for padding in some implementations that could cause information leakage. This attack is passive; the attacker can only see data that the affected device sent out as part of a packet.

Overall CVSS Score: 5.3

(AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C)

Mitigation

A firmware with the fix for this vulnerability is available for download for the SAGE 2400. As stated previously, the SAGE 2300 is beyond its End of Support and transition to SAGE 2400 is recommended.

Click here to retrieve the latest SAGE 2400 RTU firmware.

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: 2016.03.12 12:49:51 -05'00'