SAGE RTU VxWorks TCP Predictability

11-Jun-2015

Overview

Schneider Electric has become aware of a VxWorks TCP Initial Sequence Vulnerability in the SAGE RTU product line which could result in remote man-in-the-middle or denial-of-service exploitation. A software patch firmware J2 has been released remediating this vulnerability.

Vulnerability Overview

The affected devices generate predictable TCP initial sequence numbers that may allow an attacker to predict the correct TCP initial sequence numbers from previous values, which may allow an attacker to spoof TCP connections.

Product(s) Affected

The product(s) or product lines affected include:

- All SAGE RTUs using C3412 and C3413 CPU cards, all versions.
- All SAGE RTUs using C3414 CPUs with firmware versions prior to C3414-500-S02J2

Vulnerability Details

The affected devices generate predictable TCP initial sequence numbers that may allow an attacker to predict the correct TCP initial sequence numbers from previous values, which may allow an attacker to spoof TCP connections.

Mitigation

Schneider Electric has created a patch to mitigate this vulnerability on the C3414 LX-800 based RTUs. Customers may obtain this patch by contacting Schneider Electric Customer Service Department at +1-713-920-6832. Product: C3414-500-S02YZ - Secure Firmware version J2.

For all other SAGE RTU models, contact Schneider Electric Customer Service Department, +1-713-920-6832.

Schneider Electric would like to thank Raheem Beyah, David Formby, and San Shin Jung of Georgia Tech for their efforts and support in managing this vulnerability.

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=Product Security Office, email=cybersecurity@schneider-electric.com, c=US
Date: 2015.06.14 17:10:56 -04'00'