SAGE Monthly Security / Firmware Update Notice

Post Date: 7/3/2023

Summary of security related changes for June 2023.

Vulnerability Update:

- VxWorks: OS updated to version 6.9.4.12 RCPL6. Improves the protection against SSH brute force password authentication attacks by making this authentication method optional. If password authentication is enabled, a progressive time delay between incorrect SSH logins is now applied. If the default threshold of consecutive failed password logins occurs, the attempting source IP address is then banned for a period of time. Also removes low security ciphers from OpenSSL and SSH libraries.

Operational Update:

- OpenSSL: HTTPS protocol has been updated to use the OpenSSL 1.0.2.zf version.

- Webserver: Improved server-side validation of data to reduce risk of configuration data corruption.

- WEB GUI: SSH Server password authentication is now a user-defined option, disabled by default only SSH key authentication is allowed, greatly reducing risk of brute force attacks attempting to gain user access. User will enable SSH Password authentication if wanting to use this authentication method.

- DNPR: Improved network packet handling of malformed DNP3 packets.

- ModbusM: Changed size of sequential numeric break in register range that forces new data request messages to be size of 1 register, so if register 1 and register 3 are to be read, this will create 2 unique reads for register 1 and 3, instead of 1 read for 3 registers 1, 2, and 3.

Cybersecurity Update:

- SSH shell password authentication is now optional, selected by customer. Now the default authentication method is Key Pair authentication. User must enable password authentication if this feature is desired. When password authentication is enabled, a limited number of incorrect entries is allowed, with an increasing time delay between prompts for user credentials. After specific number of failures, the source IP address is banned for a period of time from making further connections.

For questions or more information contact Schneider Electric at USEnergyTS@se.com