SAGE Monthly Security / Firmware Update Notice

Post Date: 9/1/2021

Summary of security related changes for August 2021.

Security Enhancement Summary:
Firmware C3414-500-S02K5_P5 released with these enhancements:
GUI: Configuration – CPU: Additional network service checkbox provided to allow customer to enable the ISaGRAF ETCP task, which will open listening ports to connect with ISaGRAF workbench.

Configuration – CPU: Non-secure networking services Telnet and FTP are disabled by default. Customer must enable them to use them and therefore assumes risk of using them.

Security Fix Summary:
Firmware C3414-500-S02K5_P5 released to fix:
VxWorks: Vulnerability CVE-2020-28895 malloc/calloc fix. Applied Wind River patch to bring code libraries current to 6.9.4.12 RCPL3 revision. This corrects issues with overflow causing malloc/calloc to return valid pointer when it should return fail indication NULL pointer.

VxWorks: Vulnerabilities CVE-2020-25176, CVE-2020-25182, CVE-2020-25184, CVE-2020-25178, CVE-2020-25180. Provide a way for users to manually disable the comm path the ISaGRAF Workbench uses to communicate with the ISaGRAF Runtime in the RTU when not downloading new ISaGRAF RLL programs or debugging those programs. This prevents unauthorized access using this comm path.

Command Log: Fix bug where command log fails to close Syslog socket on RTU side when it detects Syslog server has closed its end. Unclosed sockets could collect eventually to point where it affects system resources, causing RTU reset.