



# SAGE Monthly Security / Firmware Update Notice

Post Date: 6/30/2021

Summary of security related changes for June 2021.

## Security Fix Summary:

Vulnerability found if using ISaGRAF functionality. Fix to resolve vulnerability currently scheduled to release by August 2021. Mitigation instructions are as follows, note that if you are not using ISaGRAF functionality the default is to have all ports disabled and there is no vulnerability.

If you are using ISaGRAF RLL programs in the SAGE RTU, the ports will be open, and the firewall will be needed to block access to those ports. If the Firewall rules are employed, you can verify they are working by trying to connect to the RTU with the ISaGRAF development system. If the Firewall is implemented and working correctly, the ISaGRAF development system will fail to connect.

Firewall rules used to block access to TCP ports 1113 and 1131:

**Schneider Electric** **K5\_P4 Update** SAGE 2400 Admin (Logout) 6/14/2021, 4:00:16 PM

[RTU Configuration](#) > [CPU Configuration](#)

**Firewall Configuration**

```
# All Firewall rules that are to be applied at system startup should be placed in this file.
# Note: All text following the "#" is a comment and ignored by the Firewall server.
#
# Example Firewall rule to filter specific IP address
# block in from 192.168.10.1 to any
#
# Example Firewall rule to filter range of IP addresses
# block in from 10.0.0.0/8 to any
#
# Example Firewall rule to filter HTTP access
# block in proto tcp from any to any port = 80
#
# Consult the Wind River Firewall and NAT setup guide for a more detailed explanation
# of Firewall configuration.
#
# Example Firewall rule to filter ISaGRAF TCP port access
block in proto tcp from any to any port = 1113
block in proto tcp from any to any port = 1131
# End of rules.
```

Cancel Submit

## Security Enhancement Summary:

No security enhancements in firmware release(s).

For questions or more information contact Schneider Electric at [sagertu\\_support@se.com](mailto:sagertu_support@se.com)