Security Bulletin ICS-VU-984947, ICSA-16-147-02

Abstract: Response for ICS-CERT Security notice

This document will help explain the necessary steps to resolve security issues discussed in the recent ICS-CERT vulnerability ICS-VU-984947 and alert ICSA-16-147-02.

Products: All BT5000 and BT6000 Series

Firmware affected: BlueX 3.6.0 to 3.8.20, and 3.9.0 to 3.9.7

Issue 1: Default users and hardcoded passwords

Some dormant Linux user accounts and hardcoded passwords could be exploited for access in some cases. There are three recommendations for resolving this issue.

1) Apply patch to handle this issue in older firmware
2) Upgrade to latest firmware, 3.8.21 or 3.9.8, available Summer 2016
3) Secure access to the unit by following general security recommendations below.

Issue 2: AT Commands can be overloaded to allow command injection

Some AT Commands will allow a malformed argument to access Linux system fundamentals. There are two recommendations for resolving this issue:

1) Upgrade to latest firmware, 3.8.21 or 3.9.8, available Summer 2016
2) Secure access to the unit by following general security recommendations below.

Resolution: Obtaining patch files

Patch files are available in .upd format and can be installed by following the upgrade methods detailed in the BlueX User's Guide. The patches are:

btsecuser_R1_bt6k.upd (Applicable for Bluex versions above 3.6.0)

btsecuser_R1_bt6k_old.upd (Applicable for Bluex versions 3.6.0 and below)

http://files.redlion.net/filedepot_download/1403/7196

This patch can be applied through BVDM or manually by AT commands with FTP file transfer.

Resolution: Upgrade to latest BlueX firmware

Please visit our website for latest version availability:

http://www.redlion.net/resources/software/sixnet-software/industrial-wireless-software-firmware

There is a new AT command, AT+BSUPWD, added to allow a user to modify the default password for the linux root user.

This AT command is documented in published doc: AT_REF_3.8.21-3.9.8.pdf

AT+BSUPWD="<Serial number of the unit>","mypassword","mypassword" this is to change root password from the default one for first time, or further change it with old password by:

AT+BSUPWD="myoldpassword","mynewpassword","mynewpassword"

Resolution: General Security Recommendations

1) Add a password for all AT command interactions
    a. AT+BRPSWD=1,6,"mypassword"
2) Set a security access level
    a. AT+BSECUR=1
    b. Available only for 3.8.16 and higher. See User Guide for more details.
3) Block access to Linux ports
    a. Use the firewall to block all access to port 6073.
    b. Make sure to disable all ACL rules first, AT+CIPACE=0
    c. Example: AT+BIPACL=1,”1.1.1.1”,”255.255.255.255”,”6073”,1
    d. Make sure to enable all ACL rules after adding rules, AT+CIPACE=1
4) Restrict access to AT Command Ports
    a. Use the firewall to restrict all access to port 5070 and 6070.
    b. Make sure to disable all ACL rules first, AT+CIPACE=0
    c. Example: AT+BIPACL=1,”x.x.x.x”,”y.y.y.y”,”5070|6070”,1
    d. Consult the User’s Guide and your IT environment for the proper ranges for x.x.x.x and y.y.y.y in your particular installation.
    e. Make sure to enable all ACL rules after adding BIPACL rules, AT+CIPACE=1
    f. Be careful! Entering invalid information may prevent any access to field units!