Honeywell

Honeywell Commercial Security
715 Peachtree St.NE
Atlanta, GA 30308
www.security.honeywell.com

October 31st, 2019

To whom it may concern;

The following information is provided in response to requests on CIP information on PW Series Controllers, parts PW6K1IC and PW6K1ICE.

CIP-007 R1
PW-Series Controllers protect against the use of unnecessary physical input/output ports used for network connectivity, console commands or removable media. Port usage is as follows:

Port#	Port Type	Usage	Can Be Disabled
67	UDP	DHCPS	No
68	UDP	DHCPC	No
80	TCP	HTTP	Yes - Use the "Disable Web Server" option on the Users web configuration page
161	UDP	SNMP	Yes - Use the "Disable SNMP" option on the Users web configuration page
162	UDP	SNMP	Yes - Use the "Disable SNMP" option on the Users web configuration page
443	TCP	HTTPS	Yes - Use the "Disable Web Server" option on the Users web configuration page
3001*	TCP	Mercury Host Protocol (MSP2)	Yes - Setting the "Connection Type" on the Host Comm page to an option that isn't IP
4001	TCP	PSIA	No
5353	UDP	Zeroconf (Discovery)	Yes - Use the "Disable Bonjour" option on the Users web configuration page

Note: The Mercury Host Protocol (MSP2) can be configured to use a different port, the default is port 3001.

CIP-007 R2.1
There have been no security patches related to PW series Controller firmware issued in the past; however, we reserve the right to do so in future should it be required. All updates to date to the Controller firmware have served to provide additional functionality or modifications to existing functionality. None of these updates are classified as security issues. Any generated patches would be referenced in the monthly Patch Management Letter. Release notes are available upon request on new firmware releases.

CIP-007 R2.2
A monthly Patch Release Letter is provided upon request via email.

CIP-007 R3.1
The PW Series controllers are implemented as a single body executable developed for a dedicated embedded application. They are not capable of accepting any external programs for execution (useful or otherwise). Therefore, the PW series controllers do not require virus protection software running on the controller. Any updates in Malicious Code prevention will be included in the monthly Patch Release Letter.

CIP-007 R4.1, R4.2, R4.3
The PW Series Controllers are not capable of logging events related to cyber security incidents that include at a minimum detected successful login attempts, detected failed access attempts and failed login attempts, detected malicious code.

CIP-007 R4.2
The PW Series Controllers are not capable of generating alerts for security events that includes detected malicious code and detected failure of event logging.
CIP-007 R4.3
The PW Series Controllers are not capable of retaining applicable event logs.

CIP-007 R5.1, R5.2, R5.5
The PW6K11C has the following default accounts:
Username: “admin”
Password: “password”

The admin user account on PW-Series Controllers is only enabled if dip switch 1 is set to on. To disable this access the recommended process is –

1. Log on to the Controller from the web interface with the default admin account.
2. Create a new admin user with a complex password.
3. Turn off dip switch 1.

The Controller should be located in a secure location to prevent unauthorized access to the DIP settings.

Web access to the Controller can be disabled by turning the feature off on the Users screen of the web interface and setting DIP switch 1 to off.

Note - If no users have been created then the default account will work regardless SW1. Once at least one user account has been created then the default account will only work with SW1 on. The option for disabling the web server is only enabled when you are logged on and SW1 is on. So you will need to have SW1 on, log on, set this option, log out, and then turn SW1 off.

The Controllers have three password Strength levels
Low Password Strength – minimum of 6 characters
Medium Password Strength – minimum of 6 characters and passes two of the password strength tests below.
High Password Strength – minimum of 8 characters, passes three of the password strength tests below, and password not based on user name.

Password Strength Tests – contains characters from any of the following categories:
Uppercase alphabet characters (A–Z)
Lowercase alphabet characters (a–z)
Arabic numerals (0–9)
Symbol characters (`! $? ^ * ( ) _ - + = { [}] : ; @ ' ~ # | < , > . /)"

The Maximum Password length is 10 characters.

The Controllers are not capable of technically enforcing password length nor complexity requirements nor technically enforcing that passwords be annually changed.

CIP-007 R5.7
The PW Series Controllers are not capable of monitoring system events related to cyber security. The Controllers are not capable of issuing automated or manual alerts for detected cyber security incidents. The controller cannot issue an alert based on unsuccessful login attempts. The Controller will lock out a web login after 3 invalid login attempts for 1 minute.

CIP-009 R1.5
The PW Series Controllers are not capable of monitoring system events related to cyber security. In the event of a Cyber Security Incident, standard Server backup and recovery procedures would apply to the PACS system to be followed if necessary by a reset and download of the PW Series Controllers.

Respectfully,

Eric Green
Sr. Global Offering Manager
George.Green@Honeywell.com