EATON CCOE SECURE CONFIGURATION DOCUMENTATION

Contents

[1 Revision History 2](#_Toc531782632)

[2 PRODUCT TEAM GUIDELINES 2](#_Toc531782633)

[3 Cyber Security Features of PX Green - Required 2](#_Toc531782634)

[3.1 Asset identification and configuration 2](#_Toc531782635)

[3.2 Restrict Physical access 3](#_Toc531782636)

[3.3 System access controls 3](#_Toc531782637)

[3.4 Secure Network Access 6](#_Toc531782638)

[3.5 Remote Access 8](#_Toc531782639)

[3.6 Logging and Event Management 8](#_Toc531782640)

[3.7 3rd Party / COTS Security 9](#_Toc531782641)

[3.8 Decommissioning or Zeroisation 10](#_Toc531782642)

[4 Cyber Security Features of PX Green - Additional 11](#_Toc531782643)

[4.1 Secure Maintenance 11](#_Toc531782644)

[4.2 Business Continuity / Cybersecurity Disaster Recovery 12](#_Toc531782645)

[4.3 Time Synchronization 12](#_Toc531782646)

[4.4 COTS Security Hardening 13](#_Toc531782647)

[4.5 Malware defenses 13](#_Toc531782648)

[4.6 Customer Application Security 13](#_Toc531782649)

[4.7 Sensitive Information Disclosure 14](#_Toc531782650)

[5 Known Issues 15](#_Toc531782651)

[6 References 16](#_Toc531782652)

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Details of Change |
| 0.1 | 25-Oct-2018 | Anurpa Jagdale | Initial Draft |
| 0.2 | 4-Dec-2018 | Anurpa Jagdale | Updated as per the Review Comments |
| 0.2 | 13-Dec-2018 | Anurpa Jagdale | Updated as per the Review Comments |
|  |  |  |  |

PRODUCT TEAM GUIDELINES

The PX Green Platform has been designed with Cybersecurity as an important consideration. Number of Cybersecurity features are now offered in this platform which if implemented as per the recommendations in this section would minimize Cybersecurity risk to product which adopts the platform. This section “secure configuration” or “hardening” guidelines provide information to the adopter team to securely develop and deploy their product using the PX Green platform to adequately minimize the cybersecurity risks to their system.

Eaton is committed to minimizing the Cybersecurity risk in its products and deploy cybersecurity best practices with latest cybersecurity technology in its products and solutions; making them more secure, reliable and competitive for the customers.

Eaton Cybersecurity Best Practices whitepapers are available that can be referenced for general cybersecurity best practices and guidelines:

***Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):***

[http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct\_1603172.pdf](http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf%20)

***Cybersecurity Best Practices Checklist Reminder (WP910003EN):*** <http://www.cooperindustries.com/content/dam/public/powersystems/resources/library/1100_EAS/WP910003EN.pdf>

Cyber Security Features of PX Green - Required

## Asset identification and configuration

Keeping track of all the devices in the system is a pre-requisite for effective management of Cybersecurity of a system. Ensure you maintain an inventory of all the components in your system in a manner in which you uniquely identify each component. To facilitate this, *the PX Green platform* supports the following identifying information - manufacturer, type, serial number, version number for application firmware and web firmware, hardware version, product name and model name. The communication settings like IP address, MAC Address, COM port, device number for each of the supported communication protocols is also supported by the platform. All this information is accessible and can be modified from the DCI sheet.

## Restrict Physical access

Attacker with unauthorized physical access could cause serious disruption to the system/device functionality. Additionally, Industrial Control Protocols don’t offer cryptographic protections at protocol level leaving the devices / systems relying on these protocols, exposed to Cybersecurity risk. Physical security is an important layer of defense in such cases. The PX Green platform is designed for use in adopter products with the consideration that it would be deployed and operated in a physically secure location.

Following are some best practices that Eaton recommends to ensure adequate security:

1. Restrict physical access to cabinets and/or enclosures containing adopter product with the PX Green platformand the associated system. Monitor and log the access at all times.
2. Physical access to the communication lines should be restricted to prevent any attempts of wiretapping, sabotage. It’s a best practice to use metal conduits for the communication lines running between one cabinet to another cabinet.
3. Utilize additional physical access restriction mechanisms such as locks, card readers, and/or guards etc. as appropriate.
4. *The PX Green platform* supports the following physical access ports, COM, Ethernet and USB. Access to them need to be restricted.
5. Before connecting any portable device through USB or SD card slot, scan the device for malwares and virus.

Eaton Cybersecurity Best Practices whitepaper provides additional information about general physical security considerations.

## System access controls

Securely configure the logical access mechanisms provided in the PX Green Platform to safeguard from unauthorized access. Eaton recommends proper use of the access controls provided in the device to restrict system access only to legitimate users. And, such users are restricted to privilege levels necessary to complete their job roles/functions. To achieve secure access control, PX Green implemented and recommends the below features

1. Ensure default credentials are changed upon first login. The product that adopts the PX Green platform should ensure to change the default credentials before it is commissioned for production. The PX Green SeedUI web page gives a user notification for changing the default password for the administrative user at first logon.
2. No password sharing – Make sure each user gets his/her own password vs. sharing the passwords. Security monitoring/logging features in the product are designed with the view of each user having his/her unique password. Security controls will be weakened as soon as the users start sharing their credentials.
3. Restrict administrative privileges - Threat actors are increasingly focused on gaining control of legitimate credentials, especially those associated with highly privileged accounts. Limit privileges to only those needed for a user’s duties.
4. Leverage the roles / access privileges to provide tiered access to the users as per the business /operational need. Follow principle of least privilege (minimal authority level required) and least access (minimize unnecessary access to system resources). The default roles defined in the platform are Admin, Engineer, Viewer and Operator. These can be changed based on adopter needs.
5. Perform periodic account maintenance (remove unused accounts).
6. Change passwords and other system access credentials no longer than every 90 days, or as per the organizational policy. In PX Green, by default, the system will enforce a 90 day age out for all user passwords. An admin user can modify or disable this password aging time from the SeedUI or REST URI POST /rs/users/accounts.
7. PX Green enforces complex passwords and session time-out, through User Management.

User management is managed in PX Green Platform as mentioned below

* User Roles with role level is defined in the REST sheet of DCI descriptors excel sheet.
* Only a user with Admin role can create/delete new users and modify configurations of other users. A user session gets created whenever a user logs in. For each session has a unique Nonce is created.
* The application and Web firmware upgrade can be done only by a user with Admin role/privileges.

There are 4 levels of Password Complexity, as defined as follows:

* Password complexity level – 0
* It should be at least 6 characters long
* It should not match with user name or full name
* It should not match with existing password
* Password complexity level – 1
* It should be at least 8 characters long
* It should not match with user name or full name
* It should not match with existing password
* It should contain at least 1 alphabetic and 1 numeric character
* **Password complexity level – 2**
* It should be at least 12 characters long
* It should not match with user name or full name
* It should not match with existing password
* It should contain at least 1 alphabetic and 1 numeric character
* It should contain at least 1 special character
* It should contain at least 1 upper case alphabetic character
* **Password complexity level – 3**
* It should be at least 16 characters long
* It should not match with user name or full name
* It should not match with existing password
* It should contain at least 2 alphabetic characters and 1 numeric character
* It should contain at least 2 special characters
* It should contain at least 1 upper case alphabetic character
* It should contain at least 1 lower case alphabetic character
* In PX Green he password are stored in encrypted NV Control of an NV Control block. The Adopters should make sure to use the NV crypto module for storing passwords in the NV control block.
* In PX Green, the password display fields are masked by character asterisk ‘\*’ and it is implemented using the DCi callback mechanism. The adopters need to make sure to implement this for the password parameters that would be added by the adopters. Refer the PX Green babel fish and its parameters.
* PX Green supports credentials type parameters to be stored in encrypted form. All these DCI parameters must have format type as $CRED and should be part of NV\_Crypto Memory block in NVM\_Address worksheet. The details can be found at the Confluence page for [Securing DCI parameters using encryption methods](https://confluence-prod.tcc.etn.com/display/LTK/Securing+DCI+parameters+using+encryption+methods).
* By default, max retry attempt for login fail is 10, but this can be changed by the Admin user by changing value of parameter DCI\_MAX\_FAILED\_LOGIN\_ATTEMPTS through REST uri or by changing the default value in DCI sheet. After the max login failed attempts, the user will be locked out for a time specified in parameter DCI\_USER\_LOCK\_TIME\_SEC.
* The SeedUI inactive session will timeout in 15minutes. User will have to login again to start the session.
* Default Authentication Method is Digest with MD5.
* Authorization Method is based on user role levels. Only users with Admin role have the all privileges to access the system. Other users with non-admin role will have limited privileges. These can be defined in the REST DCi sheet.
* Certificate Management is done through Matrix SSL using self-signed certificate.
* The default username/password is admin/ Admin\*1
* Multiple sessions of a single user is supported but not recommended and this can be configured through the DCI parameter DCI\_MAX\_CONCURRENT\_SESSION.
* PX Green supports inactivity timeout and absolute timeout for logged in User. This can also be configured from the DCI parameters DCI\_USER\_INACTIVITY\_TIMEOUT and DCI\_ABSOLUTE\_TIMEOUT\_SEC.

Logging: Audit logs supports capturing of login/logout activity. User will be locked for on reaching the limit of failure login attempt. Seed UI will display the last login time and date and number of failed attempts of the user. The number of maximum login attempts can be configured through the DCI parameter DCI\_MAX\_FAILED\_LOGIN\_ATTEMPTS.

## Secure Network Access

The PX Green platform provides network access to facilitate communication with other devices in the system. But this capability could open up a security loophole if it’s not configured securely. Following are Eaton recommended best practices for securely configuring the network access.

Eaton recommends segmentation of networks into logical enclaves and restricts the communication to host-to-host paths. This helps to protect sensitive information, critical services and limits damage from network perimeter breaches. At a minimum, a utility Industrial Control Systems network should be segmented into a three-tiered architecture (as recommended by NIST SP800-82[R3]) for better security control.

Deploy adequate network protection devices like Firewalls, Intrusion Detection / Protection devices.

* Communication Protection

The PX Green platform provides the option to encrypt the n/w traffic with HTTPS, please ensure that encryption options are not disabled. Following section details how to configure secure communication capabilities in PX Green.

By default, HTTP with digest authentication over MD5 is enabled. The Adopter should disable HTTP by default, to keep their products secure. HTTP can be disabled from the DCI sheet. In PX Green, HTTP is enabled by default.

* TLS/SSL configuration

By default TLS is enabled in PX Green. TLS can be disabled from the Prod\_Spec\_LTK\_xxx.h file, doing so will put the adopter products in a security risk

* Certificate management

The configuration related to the certificate can be found in the file Device\_Cert\_Config.h

Secure cipher suites TLS 1.2 of MatrixSSL is used, Cipher Suite 128\_CBC\_SHA is enabled with RSA key.

Currently PX Green platform does not have means to upload certificates on to the device via Web interface.

PX Green supports configuring the CORS origin header to echo the user specified domain name by default. This can be changed to use the Device IP address by setting the value of parameter DCI\_CORS\_TYPE to ALLOW\_ACTIVE\_IP to make it more secure

Please find detailed information about various Network level protection strategies in Eaton Cybersecurity Considerations for Electrical Distribution Systems [R1]. Use the below information for configuring the firewalls to allow needed access for PX Green based products to operate smoothly.

From the SeedUI Web Server, configurations related to Ethernet and IOT can be viewed from the Network tab. The SeedUI currently does not give any notification when changes in configuration are made. Adopters are recommended to make a note of this and implement it until PX Green makes this change in the SeedUI

There are parameters for each of the communication Protocol which will give the details of the IP address configurations. The parameters can be accessed using REST URI’s or through ModbusTCP/RTU.

The ports can be enabled or disabled by configuring appropriate DCI parameter values

* The DCI\_HTTP\_ENABLE DCI parameter allows enable/disable http over REST. By default it is enabled. This is another way of configuring http.
* The parameter DCI\_TRUSTED\_IP\_MODBUS\_TCP\_ENABLE allows configuring Trusted IP feature for ModbuTCP
* Similarly the parameter DCI\_TRUSTED\_IP\_HTTP\_ENABLE allows configuring trusted IP over HTTP
* After enabling IOT macro from the codebase, adopter can enable/disable IOT connection with cloud using the DCI\_IOT\_CONNECT.
* Similarly the parameter DCI\_MODBUS\_TCP\_ENABLE can be used to enable/disable ModbusTCP and parameter DCI\_BACNET\_IP\_ENABLE for BACNet IP. These can be done from the SeedUI web page as well

The DCI\_FW\_UPGRADE\_MODE allows configuration of different modes of firmware upgrade, like upgrade not allowed, upgrade to any version, upgrade to same or higher version.Whitelisting is supported by PX Green platform and by default this feature is enabled. The DCI\_TRUSTED\_IP\_WHITELIST parameter contains the list of IP addresses/range that is allowed to connect with the device. It is supported for HTTP and ModbusTCP protocols. Currently the IP address range is such that it allows all IP address. The Whitelist feature can be disabled from the EthConfig.h file.

*Note: Many compliance frameworks and cybersecurity best practices require an audit of ports and services before and after applying updates and system changes. An end user should be able to refer to the ports and services documentation to determine the expected minimal set of ports and services on a device.*

## Remote Access

Remote access to devices/systems represents a provision of control to an external party. Strict management and validation of termination of such access is vital for maintaining control over the overall ICS security.

* The PX Green platform provides the whitelist features, which allows only those IP addresses or range of IP address to connect to the board which are specified in the parameter DCI\_TRUSTED\_IP\_WHITELIST. Also the HTTPS makes it a secure connection over REST*.*
* It is highly recommended to use https configuration while transferring data over Ethernet
* The SeedUI inactive session will timeout in 15minutes, User will have to login again to start a new session.
* The CS Audit log captures the login/logout details with IP Address and Port of the user.

## Logging and Event Management

Eaton recommends that that all event and session logs are logged, including all administrative and maintenance activities. Ensure that logs are backed up, retain the backups for a minimum of 3 months or as per organization’s security policy. Perform log review at a minimum every 15 days.

* By default, Logging is disabled in the PX Green Platform. This can be enabled by uncommenting the #defines from the Prod\_Spec\_LTK\_xxx.h file. The platform supports logging on Internal and serial flash and logging on RAM. Adopters can enable any of these logging based on their hardware.
* The retention of the logs is the responsibility of the adopters, due to memory constraints; the logs are auto-deleted when the buffer becomes full.
* The types of logs and information supported are as follows:

1. Data log: Supports Change based logging and Interval Based logging for pre-defined parameters. The parameter values with time are logged.
2. Event Log: Time based event and device state is logged
3. Audit Power Log: Time based device reset and log clear events are logged
4. Audit Config Log: Status related to RAM data write operation and RAM status on device power are logged.
5. Audit User Log: Logs related to User session login/logout with user’s IP address and ports are logged. User created, deleted, password change and users blocked after max retries failed attempts are logged.
6. Audit Firmware Upgrade Log: The firmware start and end time and firmware upgrade status is logged.

* By default for Logging on RAM, data and event logs are enabled and all other logs are disabled. Adopter can configure the logs from the LogConfig.h file.
* All the logs can be exported to .csv file from the PX Green SeedUI web page.

## 3rd Party / COTS Security

Any third party component/libraries used to run software /application should not have any publicly known Critical/High vulnerabilities.

* Users are recommended to keep update the Commercial-off-the-shelf [COTS] components (e.g. an application running on Windows). It is recommended to contact the vendors for security related patches. Vulnerabilities affecting the COTS components can be tracked on National Vulnerability Database (NVD) <https://nvd.nist.gov/>.
* Users are encouraged to keep a track of the security patches released by the COTS vendors and apply them to their environment as appropriate.

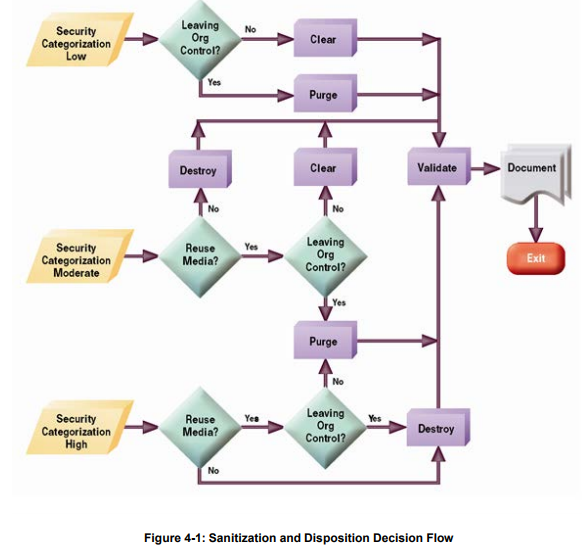
*Note: Many compliance frameworks and security best practices require a monthly vulnerability review. For many non-COTS products vulnerabilities will be communicated directly through the vendor site.*

* PX Green R10 user MatrixSSL version 3.8.7. It is recommended for the adopters to use the latest version of Matirx SSL and mbed TLS. PX Green would update to the latest version in R10 patch 1 (Dec 2018)
* The table below gives the details of all the third party components used along with their version as used in PX Green platform

|  |  |
| --- | --- |
| **Third Party Components used** | **Version** |
| BACnet - PolarSoft | 12.29 |
| EtherNet/IP - Pyramid Solutions | 4.6 |
| Profibus - profichip | 6.1.12 |
| Matrix SSL - Matrix | 3.8.7 |
| mbed TLS | 2.2.0 |
| LWIP | 1.3.2 |
| ST cube 00X | 1.5.0 |
| ST cube 10X | 1.0.4 |
| ST cube 20X | 1.1.3 |
| ST cube 30X | 1.4.0 |
| ST cube 40X | 1.7.0 |
| ST cube F7X | 1.2.3 |
| ST cube H7X | 1.0.0 |
| BLE - silabs | 2.4.2 |
| Azure - IOT | 1.30.0 |

## Decommissioning or Zeroisation

It is a best practice to purge the data before disposing any device containing data. Proper decommissioning is described in NIST SP800-88. Eaton recommends that products containing embedded flash memory be destroyed to ensure any secure data is unrecoverable.



*\* Figure and data from NIST SP800-88*

**Embedded Flash Memory on Boards and Devices**

This includes motherboards and peripheral cards such as network adapters or any other adapter containing non-volatile flash memory.

**Clear**: If supported by the device, reset the state to original factory settings.

The device can be reset to factory settings through the Modbus function code 0x42 or using the SeedUI web page or through the parameter DCI\_REST\_RESET\_COMMAND which can be accessed through the REST URI /rs/param/[pid]/value. The logs stored in the RAM will also be deleted. All these internally use the PX Green API for factory reset. To delete the logs from the Flash memory, you can hit the Delete logs button for individual log from the SeedUI. Or send the REST request DELETE /rs/log/{x}/tail.

**Purge**: If the flash memory can be easily identified and removed from the board, the flash memory may be destroyed independently from the disposal of the board that contained the flash memory. Otherwise, the whole board should be destroyed.

The internal or serial flash memory on the STM and Nucleo boards cannot be easily removed from the board, it is inbuilt with the microcontroller.

The adopter can also choose to use any other NV storage, like FRAM and dispose it accordingly.

**Destroy**: Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.

Cyber Security Features of PX Green - Additional

## Secure Maintenance

**Best Practices**

Apply Firmware updates and patches regularly

Due to increasing Cyber Attacks on Industrial Control Systems by malicious actors, Eaton implements a comprehensive patch and update process for its products in the event of new methods of compromising security of Eaton products get discovered. Users are encouraged to maintain a consistent process to promptly monitor for fresh firmware updates, implement patching and updates as and when required or released.

Whenever a PX Green release is made, all the stakeholders and adopters are notified about release and the enhanced made are documented in the release email. The adopters are encouraged to integrate the latest firmware into their products.

The contact information has been provided in the Release Notes

Eaton also has a robust vulnerability response process. In the event of any security vulnerability getting discovered in its products, Eaton patches the vulnerability and releases information bulletin through its cyber security web site - *PX Green Confluence page link:* [*http://cipt0534.nam.ci.root:8090/display/LTK/Cybersecurity+Issue+Resolution*](http://cipt0534.nam.ci.root:8090/display/LTK/Cybersecurity+Issue+Resolution)

Release Notes: http://esgit.tcc.etn.com:7990/projects/LTK/repos/babelfish/browse/Tools/RTK\_Release\_Notes.docx?at=refs%2Fheads%2Fdevelop

Conduct regular Cybersecurity risk analyses of the organization /system.

This exercise should be conducted in conformance with established technical and regulatory frameworks such as IEC 62443 and NERC-CIP.

## Business Continuity / Cybersecurity Disaster Recovery

**Plan for Business Continuity / Cybersecurity Disaster Recovery**

It’s a Cybersecurity best practice for organizations to plan for Business continuity. Establish an OT Business Continuity plan, periodically review and, where possible, exercise the established continuity plans. Make sure offsite backups include

* Backup of the latest f/w copy of *PX Green firmware*. Make it a part of SOP to update the backup copy as soon as the latest f/w is updated.
* Backup of the most current configuration.
* Documentation of the most current User List.

Save and securely store the current configurations of the device.

Following section describes the details of failures states and backup functions

* The PX Green platform supports factory reset to reset the device to default factory settings in case of device failure.
* Also a firmware fallback prevention feature has been planned for future release which would avoid firmware upgrade failure.

## Time Synchronization

Many operations in power grids, IT networks, heavily depend on precise timing information.

Ensure time synchronization provided in the device are properly configured (manual, NTP, SNTP, IEEE 1588)

The platform provide SNTP support which is documented in detail in the Release Notes -> Section 5.1 -> R9 Patch 1 Feature Description.docx -> Release R8 (RTK.1.18.1.0) Feature Details -> Section 5 SNTP Support

## COTS Security Hardening

Eaton recommends that customers Harden the platforms / products that are used to run Eaton applications / products. (eg. Dell computer, Windows Operating System, VmWare ESXi virtual host, Cisco switches, etc.)

Customers are recommended to refer COTS vendor’s documentation for guidance on Secure hardening of these components. Vendor neutral guidance is made available by Center for Internet Security <https://www.cisecurity.org/>

## Malware defenses

Eaton recommends its customers to deploy adequate Malware defenses to the platforms / products that are used to run Eaton applications / products.

Eaton Cybersecurity Best Practices whitepaper provides additional information about general physical security considerations.

## Customer Application Security

PX Green provides a platform to the customers to develop their applications according to their requirements. These applications may be developed and deployed without adequate security controls, thus opening the attack vector for the underlying device.

Eaton recommends following the below best practices to develop and host the application on the device: -

* Communication Protection: -PX Green platform provides option to develop any type of application which may need over the network communication. If application is using over the network communication, then it should be hashed and encrypted as per FIPS 140-2 standard.
* Access enforcement: - The application interface should have proper access enforcement to prevent unauthorized access to the application. Prevent unsuccessful access attempt and implement account lockout.
* Least Privilege: - The application developed by the customers should not run with root account privileges. Root account has the full control over the operating system services. If any security vulnerability occurs in application, it can compromise the complete system.
* Manual Input Checking: - All input/output in the application should be sanitized before storing and processing by the application.
* Sufficient and Minimal Error message content: - The application should generate sufficient error message to diagnose any issue in the application but shouldn’t reveal useful information that can be exploited by malicious users.
* Password Management: - Customer application should store and transmit the password in encrypted format. Password complexity should be implemented and password should be masked while setting and entering.
* Secure Coding Practices: - Follow secure coding practice while developing applications for the device.
* Remote interactive sessions: - All the remote session to the device should be encrypted, logged and monitored in the device.
* Event log generation: - The application should have the capability to log Security related events with time and date and the associated user in the device.

## Sensitive Information Disclosure

Eaton recommends that sensitive information (i.e. connectivity, log data, personnel information) which may be stored by adapter products based on PX Green platform be adequately protected through the deployment of Organizational Security Practices.

The potential Sensitive information are

* Logs stored in RAM or Flash
* User details
* Fault details

Known Issues

|  |  |  |  |
| --- | --- | --- | --- |
| **Finding No.** | **Title & Description** | **Severity** | **Recommendation** |
| CCoE\_PXGreen\_PAR\_006 | **Title: Outdated Third Party Components**  **Description:** Third Party Libraries are a major source of vulnerabilities. Product teams need to continually watchout for the vulnerabilities being reported in the components that are used in the product and should be kept up to date in order to fix security related issues. PX Green has High Severity components :  Matrix SSL  mbed TLS | Critical | This will be available in R10 Patch1 release of PX Green |
| CCoE\_PXGreen\_PAR\_008 | **Title: Authentication over Plain Text Protocol - HTTP**  **Description:** Plain text protocols such as HTTP does not offer encryption to the data stream, when sensitive information such as username, password, Auth tokens, API keys etc. are sent across network using HTTP, an attacker/user with malicious intent/ ISP/ Proxy devices could log and retrieve these information, thereby compromising the target service.    Cyber Security CCOE has identified PXGreen accepts digest authentication and its token values over HTTP. HTTPS is implemented, however the device/ web server configuration does not redirect requests received by HTTP (port 80) to HTTPS (port 443).    An attacker could simply perform Man-in-The-Middle attacks to obtain digest auth tokens, replay those valid tokens and compromise PXGreen or its adopters sharing same codebase. Once gained credentials, an attacker could perform Read/Write operation on devices | High | PX Green supports redirection to HTTPS(port 443) when HTTP is disabled. It is recommended that the adopters keep HTTP disabled by default. This can be done from the DCi sheet. |
| CCoE\_PXGreen\_PAR\_020 | **Title: Critical Change Notification**  **Description:** The system shall display warnings when critical applications or data are modified. Observation - 1) Appropriate warnings are not displayed when uploading firmware files. 2) Appropriate warnings are not displayed when changing DHCP/Manual mode, or changing IP addresses. 3) Appropriate warnings are not displayed when disabling Modbus Appropriate warnings prevent users from making unintentional errors and even detecting or identifying malicious activities making critical changes to system as hidden processes. | Medium | Adopters can implement this in their products. PX Green will implement in future releases. |
| CCoE\_PXGreen\_PAR\_022 | **Title: Vulnerability Management Plan**  **Description:** Vulnerabilities could be discovered in the product anytime during its lifecycle. It is important that the product team has a process/plan in place with details on how it will update components that have publicly known vulnerabilities against them. Ideally, this should be a regular exercise performed frequently. | Medium | Adopters need to prepare a vulnerability management plan for their products. |
| CCoE\_PXGreen\_PAR\_023 | **Title: Lack of Certificate Importing functionality**  **Description:** Vulnerabilities could be discovered in the product anytime during its lifecycle. It is important that the product team has a process/plan in place with details on how it will update components that have publicly known vulnerabilities against them. Ideally, this should be a regular exercise performed frequently. | Medium | Adopters can implement this in their products. PX Green will implement in future releases. |

References

***[R1] Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):***

<http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf>

***[R2] Cybersecurity Best Practices Checklist Reminder (WP910003EN):*** <http://www.cooperindustries.com/content/dam/public/powersystems/resources/library/1100_EAS/WP910003EN.pdf>

***[R3] NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015:***

<https://ics-cert.us-cert.gov/Standards-and-References>

***[R4] National Institute of Technology (NIST) Interagency “Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41”, October 2009:*** <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf>

***[R5] NIST SP 800-88, Guidelines for Media Sanitization, September 2006:***<http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819>