Eaton ES Product Cybersecurity CoE

IPM
Recommended Secure Hardening Guidelines

Introduction

Due to rapidly increasing Cyber Threats and cyber warfare on Industrial Control System Devices and applications, Eaton recommends following best practices for the IPM application. This section “secure configuration” or “hardening” guidelines provide information to the users to securely deploy and maintain their product to adequately minimize the cybersecurity risks to their system.

Eaton is committed to minimizing the Cybersecurity risk in its products and deploys cybersecurity best practices and latest cybersecurity technologies in its products and solutions; making them more secure, reliable and competitive for our customers. Eaton also offers Cybersecurity Best Practices whitepapers to its customers that can be referenced at www.eaton.com/cybersecurity

IPM - SECURE CONFIGURATION GUIDELINES

Category	Description
Restrict Physical access	Physical security is an important layer of defense to protect assets from various cyber security threats. IPM is developed with the consideration that it would be deployed and operated in a physically secure location. • Physical access to the systems hosting IPM and the associated applications, servers and databases should be restricted, monitored and logged at all times. • 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 to provide the communication for IPM web application and associated database and other applications. • Attacker with unauthorized physical access to the application hosting systems and servers could cause serious disruption to the application functionality. A combination of physical access controls to the location should be used, such as locks, card readers, and/or guards etc. • IPM supports the following physical access ports, o All IP capable access like Ethernet or wi-fi for remote device monitoring and IPM web user interface access o USB and serial ports for local device monitoring Access to them need to be restricted. • All devices plugged to the host system (through, but not limited to, RJ-45, USB, serial ports) have to be known and verified devices. Particularly, they shall not record or generate data from/to IPM and shall not impersonate power devices which might be monitored by IPM.
Communication Security	It is extremely important to protect all the data that is transmitted through various communication channels used in the application to safeguard the sensitive from unauthorized personals. To protect the data over these communication channels Eaton recommends following best practice for

Category	Description
	secure communication:- • Implement SSL certificate over HTTP protocol. Steps to configure the SSL certificate can be found here : IPM User Guide Chapter 15 – Appendix A / Section Cybersecurity • Disable HTTP protocol and only use HTTPS (HTTP using SSL certificate) • SSL certificate should be from a Trusted root CA and shouldn't be a self-signed certificate. • Server to server communication should be on dedicated host-to-host bases. This communication should be segregated from other communication. • Some devices provides other protocols like SNMP. Use secured versions or configurations of these protocols where available, like SNMPv3 with authentication and encryption with robust passwords instead of SNMPv1.
Database Security	IPM application uses a Sqlite database which is located on the PC on which the IPM is installed. Eaton recommends following best practices for securely maintaining the database: - • Physical Security: -Ensure physical security to the machine hosting IPM database. Physical access to these machines should be access controlled, monitored and logged all the times. • Logical access: - Restrict logical access to database on the basis of roles and permissions. Change default credentials on first use. Do not share passwords of one account with multiple people. Change password on personal change or as per the organization's password policy. • Auditing: -All kind of access to the database including administrative and maintenance activities should be logged and maintained for at least 3 months or as per organization's policy. • Backup & Restore: - Database should be properly backed up at a secure location so that it can be restored at any point of time in case of any failure. • All unused services and ports should be closed. • All file permissions should follow the principle of Least Privilege.
Restrict Logical access to IPM	It is extremely important to securely configure the logical access mechanisms provided in IPM to safeguard the application from unauthorized access. IPM provides various types of administrative, operational, configuration privilege levels. Eaton recommends that the available access control mechanisms be used properly to ensure that access to the system where IPM application is installed and to the application is restricted to legitimate users only. And, such users are restricted to only the privilege levels necessary to complete their job roles/functions. • Ensure default credentials are changed upon first login. IPM

Category	Description
	should not be commissioned for production with Default credentials; it's a serious Cybersecurity flaw as the default credentials are published in the manuals. • No password sharing – Make sure each user gets his/her own password vs. sharing the passwords. Security monitoring features of IPM are created with the view of each user having his/her own unique password. Security controls will be weakened as soon as the users start sharing the passwords. • 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. • Leverage the roles [Admin, Maintenance, Operator] provided in IPM to provide tiered access to the users as per the business /operational need. Grant privileges to users as per their job requirements; follow principle of least privilege (minimal authority level required) and least access (minimize unnecessary access to system resources). • Perform periodic account maintenance (remove unused accounts). • Change passwords and other system access credentials on personal change or as the organizations password policy. • Access to the IPM database should be restricted to the administrator of the PC or root only. • *IPM provides two levels of privileges: simple "user" who are only able to view IPM content (device list, settings, states, configuration, etc.) and administrators "admin" who are able to read and modify everything on IPM, including discovering devices, creating policies, removing protections and manage users. Ensure users have the correct level of role for their needs.* • *Users are managed locally. There is no connection to any user database like LDAP.* • *There is no password policy. Users, and particularly administrators, have to ensure their passwords meet best practices requirements (length, complexity, regularly changes).* • *By default, the primary account is named "admin". It cannot be removed before another administrator user account have been created. Changing it make attacks more difficult but administrators have to check their configuration to prevent communication loses.* • *By default, SNMP communication are SNMPv1 with "public" and "private" community names. This should be changed to SNMPv3.*
Restrict Network Access	IPM provides network access to facilitate communication with other devices in the systems and configuration. But this capability could open up a big security hole if it's not configured securely. Eaton recommends segmentation of networks into logical enclaves and

Category	Description

	restrict the communication to host-to-host paths.
	
	This helps protect sensitive information and 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,
	
	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 IPM to operate smoothly.
	
	• *Following ports are open and listened:*
	  ○ 4679 on tcp & udp *: HTTP web interface and device management protocol*
	  ○ 4680 on tcp & udp *: HTTPS web interface and device management protocol*
	  ○ 8181 on tcp : HTTP read-only REST API
	  ○ *22 on tcp: SSH server (OVA only)*
	  ○ *68 on udp: DHCP client (OVA only)*
	  ○ *123 on udp: NTP client (OVA only)*
	• *Some other ports might be open by IPM as client connections. These ports are not fixed.*

Logging and Event Management	**Best Practices**
	• Eaton recommends that that all remote interactive sessions 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.
	
	• *Logs are directly available on the web interface of IPM in the "Settings >> Log" section.*
	• *Are listed all events regarding:*
	  ○ *User management, including connections*
	  ○ *Device management including discovery and alerts*
	• *Moreover a "Export logs" command is available in the same panel to retrieve them in the form of a cvs textual Excel file.*

Secure Maintenance	**Best Practices** **Apply Firmware updates and patches regularly**

Category	Description
	Due to rapidly increasing Cyber Threats in Industrial Control Systems, Eaton implements a comprehensive patch and update process for its products. Users are encouraged to maintain a consistent process to promptly monitor for fresh firmware updates and apply the update whenever required. *Eaton regularly provides package updates of IPM directly on the web site of IPM - http://powerquality.eaton.com/support/software-drivers/.* *If an instance of IPM has an access to the internet, it regularly verifies the availability of an update and notify the user.* 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 cybersecurity web site - http://www.eaton.com/cybersecurity and patches through "IPM web site" **Conduct regular Cybersecurity risk analyses of the organization /system.** Eaton has worked with third-party security firms to perform system audits, both as part of a specific customer's deployment and within Eaton's own development cycle process. Eaton can provide guidance and support to your organization's effort to perform regular cybersecurity audits or assessments. This exercise should be conducted in conformance with established technical and regulatory frameworks such as IEC 62443 and NERC-CIP. **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 IPM. Make it a part of SOP to update the backup copy as soon as the latest f/w is updated on IPM. - Backup of the most current configurations. - Documentation of the most current User List.

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