Power and Water Cybersecurity Suite – Patch Management

Features

- Automatically identifies needed patches
- Deploys approved security patches to Microsoft® Windows® workstations and servers
- Inventories workstation operating system, software, and hardware information
- Displays patch content
- Groups endpoints for waved deployments
- Presents real-time information on a user-friendly dashboard powered by Trellix ePolicy Orchestrator®
- Discovers changes to endpoint software, hardware, and system configuration settings

Overview

Patch management is a security practice designed to address known software vulnerabilities remediated by software suppliers. Proactively managing these vulnerabilities reduces or eliminates the potential for corruption. Failure to take preventive measures ultimately increases costs through the additional time and effort expended to recover from a successful exploitation.

Software vulnerabilities are unintentionally created weaknesses in computer software programs. Malicious entities can exploit software vulnerabilities for gaining unauthorized access or privileges to computer software programs. Most successful cyber-attacks occur in unpatched systems or applications. Patches are developed to address software flaws and avoid cyber-attacks. Patching speed and accuracy is critical when taking advantage of validated, sanctioned patches. Considering the number and frequency of patch releases, manual patching can become prohibitively expensive and ineffective. An automated patching solution assists system administrators in managing software inventory and providing effective patch deployment. Patches must be pre-tested for reliable and uninterrupted deployment to a live control system. Comprehensive baseline lab testing and a waved deployment strategy prevents most undesired consequences. Additional testing with specific control system configurations simulating the production environment further enhances the robustness of the applicable patches.

Solution

Patch Management is a Power and Water Cybersecurity Suite application that employs an agent-based solution to accurately manage inventory software and determine patch needs in each system workstation and server. Patch Management uses a server tool for auditing the current state of a system and installing updates to various devices. An agent, loaded in each workstation, communicates with the server to determine device needs:

- The agent scans the host device and compiles information on the operating system, software applications, hardware devices, and services on the device.
- Results are returned to the server, and applicable patches for each device are determined.
- The agent establishes the device's patch status using the patch fingerprints.
- The server, upon receiving the device's patch status, creates and sends deployments to patch the device.
- The agent receives and installs the patches from the server.

Standard reports document patch deployments, patch status, inventory, and trends for the individual device and aggregated levels.

Operation

The core component of the Power and Water Cybersecurity Suite's Patch Management application is a server, which monitors and maintains patch compliance throughout the entire control system. Administrators access the server through a web browser. An agent is installed on every Windows station on the target network. The Patch Management application includes a dashboard powered by Trellix ePolicy Orchestrator® with the following functions:

- **Discover:** Provides asset discovery scan job functions based on a single IP address, IP range, computer name, network neighborhood, or Active Directory.
- **Review:** Reviews security contents for vulnerabilities, software packages, and discovery scan jobs.
- **Manage:** Manages system features management including endpoints, inventory, deployments, and agent policy.
- **Queries and Reports:** Generates queries and reports.
- **Tools:** Provides system administration tools such as users and roles, changing passwords, and email notifications.
- **Help:** Provides system guidance.

Compliance Summary

NERC Standard	Requirement	Emerson Response
CIP-007-6 R2 Part 2.1	A patch management process for tracking, evaluating, and installing cyber security patches for applicable cyber assets.	Emerson tracks, evaluates, and tests security patches for Windows OS, Oracle DB, Microsoft Edge, Adobe Reader, and JRE.
CIP-007-6 R2 Part 2.2	At least once every 35 calendar days, evaluate security patches for applicability.	Emerson releases sanctioned security patches at the end of each month.
CIP-007-6 R2 Part R2.3	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the	Monthly security patches easily packaged and automatically deployed to

NERC Standard	Requirement	Emerson Response
	following actions: apply the applicable patches, create a dated mitigation plan, or revise an existing mitigation plan.	Windows operating system with saved records as evidence.