U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Patch and Update Management Program for Energy Delivery Systems

A simplified process of patching and updating energy delivery system devices for end users and equipment vendors

Background

The energy sector places an emphasis on the availability and reliability of energy delivery operations. While best practice avoids the connection of energy delivery system devices to external networks, their increasing interconnectivity poses greater risk to cyber vulnerabilities. Proper and timely patches and updates are important to maintaining system cybersecurity.

For many utilities, however, the process of applying patches to energy delivery systems creates a challenge to availability and reliability as these updates sometimes require an outage. Additionally, despite careful patch testing, issues may still arise once the systems are brought back online. A patch and update management program can facilitate safer upgrades.

Barriers

- Energy sector caution to taking systems offline in order to avoid interruptions to availability and reliability.
- Devices used in energy delivery system environments increasingly share communication platforms.
- Interoperability considerations with devices from different vendors.
- Inability or lesser frequency of equipment vendors to support legacy systems with security updates.
- Level of security awareness within operational roles in energy delivery system environments.

Project Description

This project will research, develop, and demonstrate technology and techniques to identify, verify the integrity of, and facilitate deployment of patches and updates for energy delivery system software, hardware, and firmware. The project comprises several elements that can each stand alone to improve security posture, but when integrated can provide a comprehensive solution to meet energy sector patch and update needs.

A collaborative web portal aggregates and organizes patch and update information for energy delivery system devices. Prior to deploying patches, users are able to share experiences and discuss patch integrity with others in the web portal community.

The project will provide techniques and methodologies to ensure that patches are authentic, compatible, and unaltered before deployment. Validation enables end users to update devices with greater confidence of minimal impact upon availability and reliability.

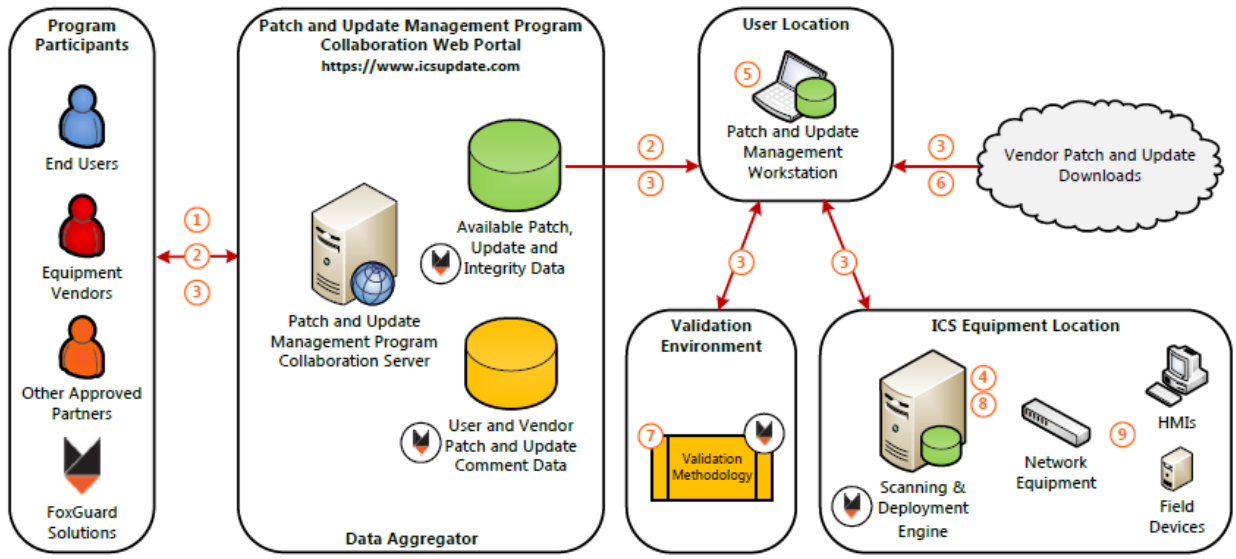
A scanning engine will provide end users with the tools to scan local and network-connected devices in order to determine their current patch level and whether they need to be updated. Upon validation of the patches, a patch deployment engine deploys the updates across the various device types.

Benefits

- Patch, update, and system vulnerability awareness
- Data repository of energy delivery system-specific patch information
- Validation techniques and methodologies to determine patch integrity prior to deployment
- Automated tools to simplify scanning and deployment of patches
- Support for legacy and state-of-the-art devices
- Crowdsourcing forums to share end user patch deployment experiences

Partners

- **FoxGuard Solutions**
- In discussion with utility and other partners



Patch and update process:

1. Log in to collaborative web portal to:
   - Research and gather available patches, updates, and integrity data for energy delivery system equipment
   - Research and share user experiences related to patch deployment
2. Download patch, update, and integrity data from web portal
3. Verify download integrity using available hash information
4. Scan control system assets
5. Compare asset listing patch level to patches, updates, and integrity data available on the web portal
6. Download required patches from designated vendor locations
7. Validate patches and updates using appropriate validation methodology
8. Deploy applicable patches and updates to assets
9. Verify deployment of patches and functionality of applicable systems

Technical Objectives

The project consists of research, development, and demonstration activities to facilitate more secure and reliable patch and update management for end users and equipment vendors. Commercialization efforts will occur alongside development activities.

Phase 1: Research and Preparation

- Engage energy sector end users to determine patch and update needs
- Acquire project equipment

Phase 2: Design and Development

- Develop end user tools, including collaborative web portal and scanning and patch deployment engines
- Define and determine validation techniques and methodologies that ensure updates behave as expected

Phase 3: Testing and Demonstration

- Conduct in-house simulation to test program functionality
- Upon agreement, demonstrate program capabilities with an end user

End Results

Project results will include the following:

- A consolidated and comprehensive approach to patching and updating multiple energy delivery system devices across equipment vendors
- Processes and techniques to verify the integrity of a patch prior to deployment
- Scanning tool to identify current patch status for energy delivery system devices
- Reliable patch deployment tools
- Anonymous and secure information sharing through the collaborate web portal

Content last updated: June 2015

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) Research and Development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of emergency disruptions due to cyberattacks.

For more information: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and

Initial Leads

Carol Hawk
Program Manager

Lindsey Hale
Contract Program Manager
FoxGuard Solutions
540-382-4234 ext. 108
lhale@foxguardsolutions.com

Current Contact as of Aug. 2020

Akhlesh Kaushiva
Program Manager
DOE CESER
202-287-6062
akhlesh.kaushiva@hq.doe.gov