

Security Guidelines for the Electricity Sector: Patch Management for Control Systems

NERC	Guideline
Guideline Title: Patch Management for Control Systems	Version: 1.0
Effective Date: 5/3/05	Approved by Board of Trustees: May 3, 2005

Preamble:

This guideline addresses potential risks that can apply to some electricity sector organizations and provides practices that can help mitigate the risks. Each organization decides the risk it can accept and the practices it deems appropriate to manage its risk.

Purpose:

The purpose of this guideline is to provide suggestions for an effective cyber security patch management strategy for control systems. A well-executed patch management program will help alleviate many of the challenges involved with securing control systems from malicious intrusion while maintaining bulk electric system reliability and high availability.

A comprehensive patch management program requires:

- current knowledge of available patches
- assessment of patch appropriateness for particular systems
- patch implementation without undesirable effects
- review of all documentation and associated procedures, such as specific configurations required
- patches are tested and installed properly
- post-implementation system observation and validation

Applicability:

This guideline is applicable to any entity that owns and/or manages control systems that support the bulk electric system.

A control system is as critical as its most critical component and is as vulnerable as its most vulnerable component. This guideline is applicable to all critical assets that are found in control centers, substations, powers plants, telecommunication systems, and all those support infrastructures that control systems depend on to operate reliably.

Each entity, using a risk assessment methodology, needs to define and identify those cyber assets it believes to be critical, keeping in mind that the ability to mitigate the loss

Security Guidelines for the Electricity Sector: Patch Management for Control Systems

of a cyber asset through redundancies or operations may make that particular asset less critical than others.

Background:

The use of non-proprietary tools and open technologies has revolutionized control systems across the electric industry. With the increased performance and openness come increased vulnerabilities. Today's control system security environment has made patch management a critical element in the reliable operation of safety-related bulk electric operations.

Having a patch management strategy does not guarantee a vulnerability or intrusion-free environment. However, a comprehensive patch management program along with other prudent cyber security practices demonstrates an entity's commitment to maintaining a secure and reliable control system environment. It assures regulators and key stakeholders that the entity is taking reasonable and prudent action in preventing malicious intrusions and maintaining reliable service.

Definitions:

Business Network — An entity's communication network, used for general purpose business activities, typically connecting a wide variety of non-critical assets and non-safety related business applications.

Control System — Those facilities, systems, and equipment that comprise the operational real-time control environment, services, diagnostics, and functional capabilities necessary for the effective and reliable operation of the bulk electric system.

Critical Assets — Those facilities, systems, and equipment, which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the bulk electric system, or would cause significant risk to public health and safety.

Guideline Statement:

A well conceived patch management program includes four fundamental features. They are:

- Control system asset inventory
- Vulnerability notification
- Risk assessment
- Implementation, documentation, and testing

All control system assets that could potentially affect the reliability of the bulk electric system need to have a formal patch management program in place and maintained. Also, the entity needs to keep records of relevant alerts, the classification of alerts, test results, implementation results, and in general sufficient documentation to describe the patch management practices that were employed.

Security Guidelines for the Electricity Sector: Patch Management for Control Systems

Guideline Detail:

Control System Asset Inventory — A successful patch management program includes a comprehensive and centralized control system asset inventory system. This program might include the detailed classification of the entity's asset pool and prioritize assets based on criticality throughout the control system environment. Each entity can use a risk assessment methodology of its choice to identify those control system assets that require inclusion in the patch management program inventory. At a minimum, all critical assets associated with control systems identified in the NERC Cyber Security Standards need to be included in the asset inventory system, with the appropriate classification and prioritization category.

A significant challenge in implementing a comprehensive and timely patch management program is the impact that the program will have on operations. The nature of control systems is such that the impact on operations, an exit strategy if unexpected results occur, and post roll-out monitoring are elements of a patch implementation plan that need to be reviewed by operations personnel. The asset inventory needs to identify those control system assets that can be patched, those that can be patched with minimal impact on operations, those that can only be patched with significant impact on operations, and those that cannot be patched. In any case, patches to critical assets associated with control systems should never be implemented by support personnel without performing a risk assessment and the knowledge of operations personnel.

Vulnerability Notification — There are many resources available to control system support personnel within the electric sector to obtain information on current vulnerabilities and the availability of patches to remediate those vulnerabilities. Subscription services are available from many hardware, software, and service providers. Each entity needs to decide which notification procedures are appropriate for their particular organization. Once the entity has completed its control system asset inventory, the following might be considered when selecting a patch notification service or methodology:

- Asset inventory (hardware and software)
- Diversity of hardware and software deployed
- Control system organization (centralized or distributed)
- Available resources

Control system support personnel that are responsible for the infrastructure, database, applications, security, and operations of the control system need to also be responsible for the patch management program associated with that control system. While control system support personnel might coordinate and communicate with their equivalent elements on the business network, the control system patch management program needs to be separate and remain unaffected by patches being applied on the business network.

Security Guidelines for the Electricity Sector: Patch Management for Control Systems

Each entity's control system patch management program needs to have a coordinator that serves as the focal point for vulnerability alert and patch management coordination within each control system environment. Patch management needs to be tightly integrated with each entity's change management practices and incident response programs so vulnerability alerts can be triaged and appropriate and timely action can be initiated. The patch management coordinator needs to be in a position to receive, evaluate, and communicate the imperative nature of each vulnerability alert.

In most cases, there is a gap in time between the issuance of a vulnerability alert and the posting of a corresponding patch. In some cases, the entity may not be in a position to integrate the patch immediately due to risk or technical limitations. In these cases, the entity's patch management program might employ the following techniques that electronically and, in some cases, physically protect the affected asset(s) from the vulnerability:

- Compartmentalization
- Defense in depth
- Temporary physical isolation or "air gapping"
- Hardened access control

Risk Assessment — Risk assessments are typically performed by a team of subject matter experts (SME) familiar with the various platforms, applications, and operations present within the entity's control system environment. The SMEs need to, as a group, be skilled in cyber and physical security, network administration, hardware support, database support, applications support, power system operations, and control system operations. The process needs to include steps to identify the risk, assess impact, and identify ownership for the appropriate resolution. Examples of risk assessment categories include:

- High impact
- Moderate impact
- Low or no impact

The entity's patch management program needs to address the acceptable time frame for a patch to be deployed based on the asset classification and prioritization category as part of the risk assessment. All risk assessments need to focus on the impact on the reliable operation of the bulk electric system and consider the risk of implementing the patch versus the risk of not implementing the patch.

Implementation and Testing — The real-time operating environment within which control systems reside presents challenges when "security" patches must be applied in a safe and timely manner. Each entity needs to have an implementation strategy for each patch or group of patches that are identified as necessary for the entity's control system

Security Guidelines for the Electricity Sector: Patch Management for Control Systems

based on other elements of this guideline. The implementation strategy needs to be proportional to the complexity and risk of impact of the patch. That is, the more risky the patch, the more comprehensive the implementation strategy. In some cases, control system suppliers might void software warranties if patches are applied without vendor approval and this needs to be avoided. In other cases, where either customized or third party systems are involved, testing and approval by multiple parties may be necessary. In either case, the patch needs to be tested by either the vendor, service provider, or the asset owner as appropriate.

Verifying that the patch performs as designed against a particular vulnerability is typically done by the vendor or service provider using sophisticated test environments and tools. Control system asset owners typically do not perform this type of testing but need to always review the test results and associated documentation. While performance testing verifies that the patch performs as designed, it does not verify that the patch is non-destructive when implemented on a given control system. This type of integration testing needs to be performed by the control system support personnel in an appropriately isolated test environment that will not affect safety related operations. The test environment needs to, as accurately as possible, emulate the production environment. Once the patch is verified to be non-destructive in a test environment, roll-out of that patch can take place after review by the appropriate operations personnel as discussed previously.

The final stage of the patch implementation strategy is post-rollout observation, verification, and record keeping. All appropriate applications, interfaces, data links, databases, etc. need to undergo a functional test and be placed “under observation” for an appropriate period of time following the successful implementation of the patch. In many cases, these verification and observation duties can be performed by operating personnel. During this period of observation, control system support personnel need to be on alert and available to respond to any latent defects that may surface.

Exceptions:

None

Certified Products/Tools:

None

Related Documents:

- *Security Guidelines for the Electricity Sector*, NERC, <http://www.esisac.com/library-guidelines.htm>
- *Urgent Action Cyber Security Standard*, NERC, August 13, 2003, ftp://www.nerc.com/pub/sys/all_updl/standards/rs/Urgent_Action_Standard_1200_Cyber_Security.pdf

Security Guidelines for the Electricity Sector: Patch Management for Control Systems

- *SP 800-40 Procedures for Handling Security Patches*, NIST, August 2002, <http://csrc.nist.gov/publications/nistpubs/index.html>
- *SP 800-30 Risk Management Guide for Information Technology Systems*, NIST, July 2002, <http://csrc.nist.gov/publications/nistpubs/index.html>
- *Overview of Attack Trends*, CERT, 2001 Carnegie Mellon University, http://www.cert.org/nav/index_red.html
- *Latest CIAC Bulletin Releases*, DOE, <http://www.ciac.org/ciac/index.html>
- *The SANS Top 20 Internet Security Vulnerabilities*, SANS, October 2004, <http://www.sans.org>
- *Patch Management Strategies for the Electric Sector*, EEI, March 2004, <http://www.eei.org>