Global Information Assurance Certification Paper

NERC CIP Patch Management and Cisco IOS Trains

GIAC (GSEC) Gold Certification

Author: Aaron Prazan, prazan@mac.com
Advisor: Rob Vandenbrink
Accepted:

Template Version September 2014

Abstract

NERC CIP Version 5 is challenging many organizations with mandatory patch management requirements. The requirements are intended to be general for any managed system with a defined source for patches or security updates. However, the picture gets muddier for Cisco network devices, because the vendor issues frequent new versions of the operating system along multiple user trains, not patches to any static version. In addition, the proprietary SCADA systems to which NERC requirements apply do not lend themselves to frequent patching. This paper will describe the requirements for patching under NERC's requirements and propose a set of processes an entity using such devices in a tightly controlled SCADA control system might use to satisfy the requirements.

1. Introduction

In April 2016, registered entities responsible for performing Bulk Electric System (BES) reliability functions as defined by the North American Electric Reliability Corporation (NERC) will be subject to a new set of standards for cybersecurity. (NERC June 26, 2015, Standards subject to future enforcement) They are the fifth version of these standards. The broadly named Critical Infrastructure Protection (CIP) standards will enforce a minimum set of security controls around cyber systems which operate the BES, and will not apply to other infrastructure elements. CIP Version 5 is not entirely new, but is a major revision of the currently enforced standards and includes many entirely new requirements, including a structured patch management process covering all devices within a protected Electronic Security Perimeter (ESP) and the devices used to control and monitor physical and logical access to the ESP. (NERC, 2015, p 15-17) All entities in the industry are working to implement the new standards and much has been written (and sold) to assist responsible entities in CIP Version 5 compliance.(NERC, 2015, June) (Tom Alrich's Blog, ERC and other topics, 2015) (SANS ICS blog | NERC CIP is hard! | SANS Institute, 2015)

Patch Management is a cornerstone of today's defense in depth strategy. It is an implementation step in three of the twenty SANS Critical Security Controls (SANS, 2015, July, controls 3,6, & 10); NIST also provides excellent guidance in its SP 800-40 publication (Souppaya & Scarfone, 2013) and virtually no-one in the IT world suggests not patching for new vulnerabilities. However, it is not uncommon for vendors of custom-built SCADA systems to either instruct their customers to not patch certain elements of the system or to be very conservative, patching only after extensive testing on a vendor-owned test system, and then again on the system owner's test system. Even then, it is impossible for a vendor or owner's test system to completely duplicate the critical production system to which virtually zero downtime is acceptable and frequent patching is done at the owners' peril.

Furthermore, the SCADA vendor may guarantee support only for the servers, databases, and user interface software, leaving network infrastructure management up to the owner. Complying with a strict and frequent patching program is therefore an

operational risk, while not complying is a compliance risk subject to financial penalties up to $1M per day per infraction. (42 U.S.C., 2005)

Finally, the patching model in use by the market leader, Cisco (IDC, 2015), does not lend itself well to the patching model laid out in the CIP Version 5 requirements because the company does not actually release any patches to their major software, Cisco IOS. Instead of patches, the company releases a complicated set of new versions of IOS meant for different types of users, which they call "trains," and does so quite frequently (Rullan, J, 2005). The company also releases Security Advisories, Security Responses, Security Alerts, Bug Reports, Software Advisories, Field Notices and other communications to assist customers in choosing the right train and right version for their environment. This ever-growing body of published material makes it challenging to know how, exactly, to evaluate and document "security patches" to IOS software for compliance purposes.

This paper is meant to summarize the NERC CIP Version 5 requirements, the Cisco versioning process, and propose some possible processes which entities could use to comply.

2. Discussion

2.1. NERC CIPv5

Designed as a minimum level of protection against malicious cyber attacks and accidental incidents, the security controls in the NERC CIP standards require performance of activities that are recognized as best practices in the IT industry. The goal of the standards is to ensure the reliable operation of the Bulk Electric System in North America, recognizing that at some level this depends on protection of the control systems from accidental misoperation and malicious cyber attacks.

The standards themselves are a product of a Standards Drafting Team that is made up, mostly, of people working in the electric industry. New standards are subject to an approval process which includes voting by the entities in the industry which must then follow the requirements in the standards. The most recent major revision (Version 5) was approved by the Standards Drafting Team, industry member votes, and the Federal

Energy Regulatory Commission, and will become effective in April 2016. Industry is working at all levels to transition from the older version the reliability standards (Version 3) to Version 5.

2.1.1. NERC CIP Patch and Change Management

Patch Management in Version 5 is an iterative process designed to give asset owners flexibility while ensuring they do not miss security patches that are made available through known vendor distribution channels. The process is as follows for identified systems to which the standards apply (NERC, 2015, p. 15-17):

1. "[Identify] a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists."
2. "At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified [in step1.]"
3. "For applicable patches identified [in Step 2], within 35 calendar days of the evaluation completion, take one of the following actions:
   - Apply the applicable patches; or
   - Create a dated mitigation plan; or
   - Revise an existing mitigation plan.

   Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations."
4. "For each mitigation plan created or revised [in Step 3], implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified [in Step 3] is approved by [a designated company Officer] or delegate."

As written, an entity could follow a monthly patching program or defer patching to a planned maintenance period in the future: quarterly, semi-annually, or other time period. However, it should be noted that NERC CIP is an evidence-based standard subject to

rigorous audit. The system owner must be prepared provide documented evidence to answer any question about the patching process and activities, such as "Please show me dated screen shots or system logs showing application of all patches evaluated for asset numbers on this list for the period March 1 – May 31, 2013, and any mitigation plans used or in use to schedule those patches." A chosen process must result in the creation of evidence of that detail (or better.)

Other details to consider are mandatory documentation of change control approvals, testing and monitoring for unauthorized changes to applicable Cyber Systems (quoted or paraphrased from the standard NERC CIP-010-1 in Figure i).

Figure i Process and Evidentiary Requirements for Patch Application, in addition to CIP-007 R2

- Monitor at least once every 35 calendar days for changes to the baseline configuration (which includes application of security patches).
- Authorize and document changes that deviate from the existing baseline.
- Document and investigate detected unauthorized changes.
- Update the baseline within 30 days of completing the change
- For a change that deviates from the existing baseline configuration:
    - Prior to the change, determine required cyber security controls that could be impacted by the change;
    - Following the change, verify that required cyber security controls are not adversely affected;
    - Where technically feasible, test the changes in a test environment or production environment where test is performed in a manner that minimizes adverse effects, that models the baseline to ensure required cyber security controls are not adversely affected.
    - Document the results of the testing, verification and differences between the test environment and production environment, including measures used to account for any differences in operation between test and production environments.

It is easy to see why system administrators may be challenged to apply patches monthly and still comply with the requirements, including documentation proving compliance for audit purposes. Appendix Figures iv and v graphically depict the minimum required process flows for NERC CIP patch and change management in an Electric Control Center environment.

Aaron Prazan, prazan@mac.com

2.2. Cisco Patch Releases

Cisco releases security patches neither for its flagship network switch software, Cisco IOS, nor appliance software for its widely used security gateways. Instead, it releases entirely new versions of these operating systems on a frequent schedule, announcing changes in a weekly Software Update, sent at 10am each Sunday morning. Is NERC CIP patch management simply not applicable? No, NERC does not accept the argument that patches don't exist, and even if they did, vulnerability assessment and mitigation requirements would force even the most conservative system owner to evaluate and apply appropriate updates periodically.

Evaluation is complicated due to the large number of options available for a given product. For example, Catalyst 3750X-24P-L switches received new IOS releases in April and May, 2015. Latest available IOS versions for that switch model were listed on July 14, 2015 as:

- 15.2.3E1 (April 30, 2015)
- 15.0.2-SE8(MD) (May 25, 2015) (suggested based on software quality, stability, and longevity)
- 12.2.58-SE2(ED) (July 27, 2011)
    - *Plus 34 other available supported versions! (see Appendix Figure iii)*

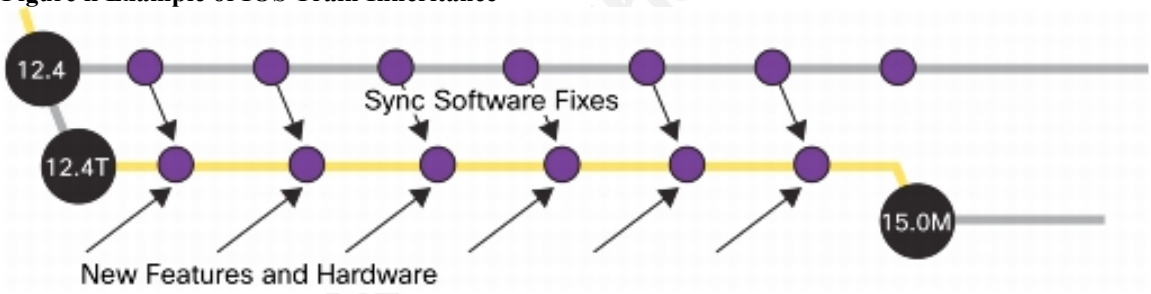
Why is the latest version 15.2.3E1 not suggested? What is meant by E, SE, MD? If an entity were running anything other than these, is an upgrade required?

The answer lies in Cisco's use of product release families called trains. Each train starts with a common code base: a mainline release which can be thought of as a version. In our example, we are dealing with mainlines, or versions, 12.2, 15.0, and 15.2. New releases within a mainline incorporate fixes to bugs and security vulnerabilities. Thus, release 15.0.2 may have security patches compared to 15.0.1. MD signifies the release has been widely tested and is "maintenance deployable." Though 15.0.2 received new features as recently as May 25, its underlying mainline code has been shown to be stable over a long period.(Cisco, 2010) 15.0.2 was first released in August 2012 and received new features, but no fixes, since. ED signifies Early Deployment with new features, platform, or

interface support. (Cisco, n.d.) The ED release of 12.2.58 may be a release of an older code base that supports newer hardware.

Releases are further segmented according to the needs of different market segments. The segmented groups are the trains, and will contain both fixes inherited from the mainline and new features incorporated for specific user bases. Trains are designated by capital letters, E for enterprise, S for service provider, T for technology user, B for broadband or leased line aggregator and so on. New features added to a user train are not added to the mainline, but may migrate to the next mainline when it is released. The latest release to a train contains the most current fixes, so 15.0.2-SE8(MD) users do not have a security justification to migrate to 15.2.3E1, but may want the features incorporated into 15.2. The number after the train signifies the rebuild number within that train. Figure ii illustrates this.

Figure ii Example of IOS Train Inheritance



2.2.1. Version Number Guidelines

For the entity looking to evaluate patches on a frequent basis, some general guidelines follow from analysis of the version numbers. One is to consider new releases within one's currently installed mainline and train. If you're running 12.2.58 and a new release occurs in 15.0.2, it's not relevant. Also, updates to the train but not the mainline should include features, not fixes. 15.0.2-SE7 is not likely to have major security patches compared to 15.0.2-SE6, but running 15.0.1 may prompt more investigation to see what changed.

2.2.2. Cisco Release Notes

Each release comes with release notes. These are copious; the recommended version in our example15.0.2-SE8(MD) weighs in at 84 pages.(Cisco, 2015) Much of it can be ignored for the purpose of patch evaluation, however. There is a section on new features,

which may be of interest, but the key is found at the end, in the section titled "Caveats Resolved in Cisco IOS Release 15.0(2)SE8." There are listed 33 bug fixes resolved from SE7→SE8. Many of these are extremely specific to a specific user's reported environment such as "Switch sent Failure packet after reboot and caused PC to fail to authenticate."(Cisco, 2015, Bug Search > CSCuo66933) Many are specific to other hardware such as Cisco 2960 or 3560X switches. Some look like possible security concerns such as "LOGIN_FAILED log message should not display the bad username" or "Switch crashes with multicast routing enabled when TCN timer expires" (Cisco, 2015, Bug Search > CSCur94665) There is documentation for each caveat in Cisco Bug Descriptions. Many will be inapplicable to the owner's environment, and most have a workaround that mitigates the bug without migrating to the new version. In the case of CSCur94665, the crash problem is mitigated by a workaround to "disable Spanning tree in all the VLANs to avoid STP TCN." (Ibid) Of course, if VLANs are not implemented, then there is no reason to migrate to the new version.

2.2.3. Documenting A Patch Evaluation For CIP Compliance

Practices to document an evaluation could vary from light to detailed analysis, but should be consistently applied to show the policy is repeatable. Ideally, one configuration would be in standard use, so that one evaluation covers all assets in the environment. If not a separate evaluation is necessary for each configuration.

At minimum, scan release notes for caveats that cite known vulnerabilities or Common Vulnerability and Exposures (CVE) numbers. Minor changes to features or bugs experienced by a small number of users would not reference these. Also, publication of a Cisco Security Advisor or Security Notice indicates vulnerabilities. Releases not accompanied by such a notice are probably not security concerns. A more rigorous, but much more time consuming, practice would be to tabulate all the caveats treated by the release and document an evaluation for each. An example is shown in Appendix Table 1 for the latest release of 15.0.2-SE8(MD). None of the caveats references a vulnerability, and noting this alone would be sufficient for minimum compliance.

Cisco's does not always strictly follow its process adding security patches to the mainline and features to the train. Reasons for this are not clear, but to the user the

process steps are unchanged. If caveats reference known vulnerabilities, they still must be evaluated for applicability to the production environment. For example, a caveat resolved in Cisco IOS Release 15.0.2-SE1 was:

> CSCtg47129: The Cisco IOS Software implementation of the virtual routing and forwarding (VRF) aware network address translation (NAT) feature contains a vulnerability when translating IP packets that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition.(Cisco, 2015, Bug Search > CSCtg47129) CVE-2013-1142 (NIST, 2013)

If the production environment used switches to NAT addresses between segments, administrators would be obligated to either apply the update or create a mitigation plan that schedules its application in the future, or cite other mitigations that make it unnecessary. An example of mitigations would be use of monitoring for CPU usage, a symptom of exploitation described in the release notes and bug search associated with CSCtg47129. Of course, if the feature was not implemented in production, the vulnerability is not applicable there would not be a reason to apply the update.

Entities following NERC CIP have an obligation to document each evaluation of new releases for each applicable system. Required documentation also includes dated mitigation plans, revisions to dated mitigation plans and all items in Figure i.

With the frequency that Cisco releases new versions of software for its products, it is certain that some vulnerabilities will be addressed that are applicable to the production environment. However, SCADA control systems cannot be patched quickly. Even with the decision to patch on day one, the steps required for performing and documenting testing required under NERC CIP-010 could take more than 35 calendar days. Another process for ensuring compliance and production reliability is to schedule patches independent of software releases. Committing to upgrade to the latest version in the train captures all the caveats of prior versions and overrides the 35 day deadline imposed by the standard. For each new release, document a review whether it is very detailed or addresses only references to known vulnerabilities, and add it to a mitigation plan which includes a scheduled upgrade. There is no requirement to patch within a quarter, half or even full year, only that it be a dated mitigation plan that mitigates the

vulnerabilities addressed by the patch and that it be completed within the timeframe stated in the plan. The standard even allows for the revision of previous dated mitigation plans if they cannot be performed within the original timeframe. As long as the applicability evaluation is performed and documented faithfully every few weeks, not to exceed 35 days from the last evaluation, and a record of mitigation plan dates is maintained, compliance is assured. This diligence also ensures that no security fixes are missed, and that consideration is given to unpatched vulnerabilities. The standards are rigorous, but on this point, provide flexibility.

3. Conclusion

NERC CIP requirements for patch management are a new framework for Bulk Electric System asset owners which reflects recognized best practices. The framework is mandatory, documentation intensive, auditable, and subject to financial penalties if not followed. Application of these requirements to network devices seems especially challenging because their patch structure is frequent and complex. However, analysis of the Cisco release structure shows that it is designed around new features for a diverse worldwide user base and from a security perspective can be understood discretely. Release documentation, while lengthy, can be reviewed with minimal effort to isolate treatment of known vulnerabilities. Patch requirements, while exacting, are flexible to the realities of a production SCADA environment and a set of best practices are proposed to allow system owners to comply with NERC CIP, take full advantage of security work performed by Cisco, and maintain sanity.

A process requiring minimal effort which maintains compliance and ensures the entity incorporates relevant security fixes is described. The process requires diligence to evaluate new releases and vendor release notes, but uses the NERC standard requirement for mitigation dated plans to allow the entity to schedule network maintenance when it is operationally feasible, and when all necessary compliance activities for testing and change control can be documented.

Aaron Prazan, prazan@mac.com

References

42 U.S.C. (2005). *Energy Policy Act of 2005* (Sec 15801-16524). Washington, D.C.: U.S. G.P.O.

Cisco. (2010, July). Cisco IOS Software Release 15 M and T Q&A - Cisco. Retrieved from http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-software-release-15-0-1-m/qa_c67_561940.html

Cisco. (2015, May 20). Release Notes for Catalyst 3750-X, 3750-E, 3560-X, and 3560-E Switches, Cisco IOS Release 15.0(2)SE and Later - Cisco. Retrieved from http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/15-0_2_se/release/notes/OL25302.html

Cisco. (2015, July 13). Bug Search > CSCuo66933 Switch Sent Failure Packet After Reboot And Caused PC to Fail Authen. Retrieved from https://tools.cisco.com/bugsearch/bug/CSCuo66933/?referring_site=ss

Cisco. (2015, July 15). Bug Search > CSCur94665 Switch Crashes With Multicast Routing Enabled When TCN Timer Expires. Retrieved from https://tools.cisco.com/bugsearch/bug/CSCur94665/?referring_site=ss

Cisco. (2015, July 15). Bug Search > CSCtg47129 NAT Memory Leak Vulnerability. Retrieved from https://tools.cisco.com/bugsearch/bug/CSCtg47129/?referring_site=ss

Cisco. (n.d.). Cisco - Release Designations Defined. Retrieved from http://www.cisco.com/warp/customer/417/109.html

IDC. (2015, June 3). IDC's Worldwide Quarterly Ethernet Switch and Router Trackers Show Ethernet Switch Market Flat to Slightly Positive, Growth Indicators for Router Market - prUS25642515. Retrieved from http://www.idc.com/getdoc.jsp?containerId=prUS25642515

NERC. (2015, June 26). CIP Standards. Retrieved from http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx Subject to future enforcement

Aaron Prazan, prazan@mac.com

NERC. (2015). *CIP-007-5 Cyber Security - System Security Management*. Retrieved from http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-007-5&title=Cyber Security - System Security Management&jurisdiction=null

NERC. (2015, June). Implementation Study, Lessons Learned, and FAQs. Retrieved from http://www.nerc.com/pa/CI/Pages/Transition-Program-V5-Implementation-Study.aspx

NIST. (2013, March 28). Vulnerability Summary for CVE-2013-1142, National Vulnerability Database. Retrieved from https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-1142

Rullan, J. (2005). *Understanding Cisco IOS Naming Conventions*. Paper presented at Cisco Academy Conference. Retrieved from http://www.cisco.com/web/learning/le21/le34/downloads/689/academy/2005/BRK-101.pdf

SANS Industrial Control Systems Security Blog | NERC CIP is hard! | SANS Institute [Web log post]. (2105, July 8). Retrieved from http://ics.sans.org/blog/2015/07/08/nerc-cip-is-hard

SANS. (2015, July). SANS Institute - Critical Security Controls. Retrieved July 5, 2015, from https://www.sans.org/critical-security-controls/

Controls 3, 6, and 10

Souppaya, M., & Scarfone, K. (2013). *Guide to Enterprise Patch Management Technologies* (SP 800-40 Rev 3). Retrieved from NIST website: http://dx.doi.org/10.6028/NIST.SP.800-40r3

Tom Alrich's Blog: ERC [Web log post]. (2015, July 7). Retrieved from http://tomalrichblog.blogspot.com/2015/07/erc.html

Aaron Prazan, prazan@mac.com