The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Patch Management Mitigation Plans

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity strive to improve your compliance posture and work toward continuous improvement in the reliability, security, resiliency, and sustainability of your CIP compliance programs.

There are times that I may also discuss areas of the standards that other entities may be struggling with and share my ideas to overcome their known issues. As with lighthouses, I can't steer your ship for you, but perhaps I can help shed light on the sometimes stormy waters of CIP compliance.

Q I have several BES Cyber Assets that cannot be patched. Is it possible to have a patch management mitigation plan in place that does not need to be updated with every patch that is released for these systems?

A CIP-007-6 R2 (Security Patch Management) requires a new or revised patch management mitigation plan for each and every applicable security patch that is not applied within the time window specified. Note that there are two types of mitigation plans that may apply to the CIP Standards (see sidebar, "Two Types of Mitigation Plan"). In this article, I will review how mitigation plans fit into a vulnerability management program and what the expectations are for those mitigation plans. I will also discuss some methods that might be used to make a mitigation plan easier to adapt to new vulnerabilities.

Two Types of Mitigation Plan

The "mitigation plan" (not capitalized) referenced by CIP-007-6 R2 should not be confused with the term "Mitigation Plan" (capitalized) defined in the NERC Rules of Procedure. As used in this article, "mitigation plan" refers to a plan used to mitigate a vulnerability, not a Plan to correct and prevent re-occurrence of a violation.

Vulnerability Management

In a vulnerability management program, a mitigation plan fills the security gap between the identification of a vulnerability and the vulnerability's removal from an affected system. A vulnerability is removed by modifying the software containing the vulnerability.

For more information about vulnerability management programs, see The Lighthouse in the July/August 2016 issue of the RF Newsletter.

This is usually done by applying a security patch, but may also be accomplished by upgrading to a version of software that does not contain the vulnerability or by removing the vulnerable software from the affected system. In any case, if the vulnerability cannot be removed in a timely manner it must be mitigated by a series of actions contained in a mitigation plan.

CIP-007-6 R2 addresses only those vulnerabilities that enter your vulnerability management program by way of the release of a security patch, but in my opinion you will best serve the needs of reliability by identifying all vulnerabilities that may impact your systems. Whether you implement a full vulnerability management program or stick with a basic patch management program, one of your primary sources for vulnerability identification will be security patches.

Eagle River, MI - Photo: L. Folkerth

CIP-007-6 R2 requires you to evaluate each security patch for applicability and within 35 calendar days of this evaluation apply the patch, create a new mitigation plan, or modify an existing mitigation plan.

Lifecycle of a Patch Management Mitigation Plan

A mitigation plan has several stages in its existence:

Creation – A mitigation plan is created in response to the release of a security patch that can't be applied within 35 days of the evaluation of the patch for applicability. The mitigation plan must include planned actions and a timeline.

Modification – This stage of the mitigation plan is optional. If the mitigating actions required for a newly released patch are similar to those of a previously mitigated patch, you may want to modify an existing mitigation plan rather than start a new one from scratch.

Mitigation Plan Approval – If a mitigation plan is modified, the modifications must be approved by the CIP Senior Manager or specified delegate. It would be prudent, although not required by CIP-007-6, for management to also review, assess, and approve new mitigation plans.

Continued on page 15

Continued from page 14

Execution – After a mitigation plan is created, the plan is executed to implement the mitigating actions specified by the plan.

Revision and Approval – If the mitigating actions are not completed by the dates specified in the plan's timeline, a new timeline must be developed and approved by the CIP Senior Manager or a specified delegate. Be aware that multiple extensions or a substantial extension of the timeline may be closely scrutinized by your audit team. You should carefully document the reasons for any timeline changes.

Completion – When all of the mitigation plan's mitigating actions have been performed, the mitigation plan is considered complete.

Maintenance – Once the mitigation plan is complete, ensure that any configuration items or other mitigating actions are not undone by subsequent changes. One way to accomplish this is to periodically monitor any configuration items that were changed by the mitigating actions. Changes to these configuration items need to be reviewed to verify they did not weaken the mitigations.

Termination – Vulnerabilities may be removed from applicable systems by several methods:

- patching the vulnerable software;
- upgrading the software to a version that does not have the vulnerability;
- uninstalling the vulnerable software; or
- decommissioning the Cyber Asset that contains the vulnerable software.

After all vulnerabilities covered by the mitigation plan are removed from all applicable systems, then the mitigation plan may be terminated and maintenance of the plan may cease. Remember to keep all of your documentation of the mitigation plan's implementation as audit evidence.

Expectations of a Patch Management Mitigation Plan

For the purposes of CIP-007-6 R2, I suggest a mitigation plan structure that consists of eight parts:

1. Identification of the vulnerability or vulnerabilities addressed.

   The mitigation plan should begin by listing the vulnerabilities it applies to. This can be accomplished by listing the patch that fixes the vulnerability, or by providing the National Vulnerability Database (NVD) identifier. Be aware that the NVD usually contains a Common Vulnerability Scoring System (CVSS) Severity Score that can be helpful in determining the overall risk presented by a vulnerability. This can be useful when assessing risk, as described in part 3 below.

2. Identification of the systems or types of systems affected.

   At a minimum, you should record the in-scope systems that have this vulnerability. You will want a control in place to ensure that vulnerable systems are not missed. An automated tool can assist here.

   As a part of your list of affected in-scope Cyber Assets it may be useful to keep the patch status of each system and the date patched. This ensures all information about the vulnerability is in the same place.

3. Consideration of the methods that might be used to exploit the vulnerability.

   This is where you begin developing your mitigating actions. Identify the means an attacker might use to take advantage of the vulnerability in your networks. By considering how a vulnerability could be exploited, you will also identify the risks to your systems. Documentation of these risks can be used in other phases of the mitigation plan to help in establishing prioritization, timing, resource allocation, etc.

4. Mitigating actions to prevent the exploits from occurring.

   From your analysis of the possible attack vectors in step 3, develop a list of configuration items to change and other actions you will take to protect your affected systems. Note that these protections need not be the same for each system, but may reflect different levels of risk based on the location of the system, the function of the system, and other factors.

5. Action items to implement.

   Develop action items and document how you will implement the mitigating actions. Each action item should be a discrete task that can be identified and tracked.

6. Target dates for each action item.

   Assign completion targets for each action item or task. These target dates should reflect the risk posed by the vulnerability and the possible exploits. High risk items should receive immediate attention. Lower risk items can be scheduled when resources are

Continued on page 16

Continued from page 15

available. While CIP-007-6 R2 doesn't specify a timeframe for implementation of the mitigation actions, you must be able to demonstrate to an audit team that your implementation dates are prudent. In my opinion, a good guideline to use would be to mitigate high risk vulnerabilities within a couple weeks of discovery, while it might be reasonable to allow very low risk items to go as long as three months. Whatever approach you take, be sure you document your risk-based approach to determining target dates.

7. Monitoring steps.

   You should maintain a list of configuration items that will be monitored to ensure the mitigating actions remain in effect until the vulnerability is removed from all target systems.

8. Conditions upon which the mitigation plan may be terminated.

   You should list the patches that need to be applied in order for the mitigation plan to be terminated. If a software upgrade is expected to remove the vulnerability, list the minimum version of the software that is required. Or, if it will take a complete system replacement to remove the vulnerability, that should be stated. This information will enable you to determine when the mitigation plan may be terminated (see Lifecycle above).

Note that if you employ an automated patch management system, you may be able to extract much of the required information from that system.

Improving the Coverage of an Existing Patch Management Mitigation Plan

The actions I propose above for a mitigation plan involve a substantial amount of work. If you are in the situation where you are not able to patch systems within the 35-day window, then you will need to become very efficient at developing, implementing, and monitoring mitigation plans. This may include patching delays of:

- Several weeks (e.g., the systems are in a transmission substation and you can't touch them during peak load season),
- Several months (e.g., you need a generating plant scheduled outage of several days to be able to patch), or
- Several years (e.g., a previous patch can't be applied because it interferes with the functioning of the system and subsequent patches are cumulative, so you need a "fork-lift" upgrade to fix the vulnerability).

One way of becoming more efficient might be to categorize mitigation plans by the type of vulnerability addressed. For example, your mitigation plans for Microsoft Server Message Block (SMB) vulnerabilities may contain similar actions. If you already have a mitigation plan that addresses SMB vulnerabilities, it might be easier to modify that plan rather than start a new one from scratch. It is possible you may only need to update the applicable patches and reconsider the possible attack vectors.

Keep in mind that even if you don't need to take any additional mitigating actions because the ones you have in place are effective against exploits of the new vulnerability, you still must revise the mitigation plan. The plan needs to reflect the new patches and any new vulnerabilities identified, even if the mitigating actions are the same.

Requests for Assistance

If you are an entity registered within RF and believe you need assistance in sorting your way through this or any compliance related issue, remember RF has the Assist Visit program. Submit an Assist Visit Request via the rfirst.org web site here.

Feedback

Please share any feedback you may have on these articles. Suggestions for topics are always appreciated. I may be reached here.