NIST SPECIAL PUBLICATION 1800-31A

Improving Enterprise Patching for General IT Systems:

Utilizing Existing Tools and Performing Processes in Better Ways

Volume A:
Executive Summary

Alper Kerman
Murugiah Souppaya
Kevin Stine
National Cybersecurity Center of Excellence
Information Technology Laboratory

Mark Simos
Sean Sweeney
Microsoft
Redmond, Washington

Karen Scarfone
Scarfone Cybersecurity
Clifton, Virginia

FINAL

April 2022

This publication is available free of charge from
https://doi.org/10.6028/NIST.SP.1800-31

The draft publication is available free of charge from
https://www.nccoe.nist.gov/publications/practice-guide/nist-sp-1800-31-improving-enterprise-patching-general-it-systems-draft

Executive Summary

For decades, cybersecurity attacks have highlighted the dangers of having computers with unpatched software. Even with widespread awareness of these dangers, however, keeping software up-to-date with patches remains a problem. Deciding how, when, and what to patch can be difficult for any organization. Each organization must balance security with mission impact and business objectives by using a risk-based methodology. To address these challenges, the NCCoE has collaborated with cybersecurity technology providers to explore approaches for improving enterprise patching practices for general information technology (IT) systems. These practices are intended to help your organization improve its security and reduce the likelihood of data breaches with sensitive personal information and other successful compromises. The practices can also play an important role as your organization embarks on a journey to zero trust.

CHALLENGE

There are a few root causes for many data breaches, malware infections, ransomware attacks, and other security incidents, and known—but unpatched—vulnerabilities in software is one of them. Implementing a few security hygiene practices, such as patching operating systems, applications, and firmware, can prevent many incidents from occurring, lower the potential impact of incidents that do occur, and increase the cost to the attacker. Unfortunately, security hygiene is easier said than done. Despite widespread recognition that patching is effective and attackers regularly exploit unpatched software, many organizations cannot or do not adequately patch. There are myriad reasons why, not the least of which are that it's resource-intensive and that the act of patching can reduce system and service availability. Many organizations struggle to prioritize patches, test patches before deployment, and adhere to policies for how quickly patches are applied in different situations. Delaying patch deployment gives attackers a larger window of opportunity.

This practice guide can help your organization:

- overcome common obstacles involving enterprise patching for general IT systems
- achieve a comprehensive security hygiene program based on existing standards, guidance, and publications
- enhance its recovery from incidents that occur, and minimize the impact of incidents on the organization and its constituents

SOLUTION

To address these challenges, the NCCoE has collaborated with cybersecurity technology providers to develop an example solution. It demonstrates how tools can be used to 1) implement the inventory and patching capabilities organizations need to handle both routine and emergency patching situations, as well as 2) implement isolation methods or other mitigations as alternatives to patching. The solution also demonstrates recommended security practices for patch management systems themselves.

The NCCoE assembled existing commercial and open source tools to aid with the most challenging aspects of patching. The NCCoE built upon previous NIST work documented in *NIST Special Publication (SP) 800-40 Revision 3, Guide to Enterprise Patch Management Technologies* and *NIST SP 800-184, Guide for Cybersecurity Event Recovery*.

Collaborator	Security Capability or Component
Cisco	Asset discovery and inventory; network access control; network policy enforcement
eclypsium	Hardware and firmware inventory; firmware vulnerability assessment; firmware integrity monitoring; firmware updates
FORESCOUT	Asset discovery and inventory; security policy enforcement
IBM	Asset inventory; configuration management; software updates; vulnerability scanning of source code as part of a DevOps pipeline
Lookout	Security policy enforcement; vulnerability scanning and reporting; software discovery and inventory; firmware vulnerability assessment and policy enforcement
Microsoft	Asset discovery; configuration management; software updates
tenable	Asset discovery and inventory; vulnerability scanning, reporting, and prioritization
vmware	Vulnerability scanning and remediation; configuration management; software updates

While the NCCoE is using commercial and open source products to address this challenge, the practice guide will not endorse these particular products, nor will it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

HOW TO USE THIS GUIDE

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief information security and technology officers can use this part of the guide, *NIST SP 1800-31A: Executive Summary*, to understand the drivers for the guide, the cybersecurity challenge we address, our approach to solving this challenge, and how the solution could benefit your organization. Business decision makers can also use *NIST SP 800-40 Revision 4, Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*. It complements the implementation focus of this guide by recommending creation of an enterprise strategy to simplify and operationalize patching while also reducing risk.

Technology, security, and privacy program managers who are concerned with how to identify, understand, assess, and mitigate risk can use *NIST SP 1800-31B: Security Risks and Capabilities,* which describes what we built and why, including the risk analysis performed and the security capabilities provided by the example implementation. *NIST SP 800-40 Revision 4, Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology* may also be helpful.

IT professionals who want to implement an approach like this can make use of *NIST SP 1800-31C: How-To Guides*, which provide specific product installation, configuration, and integration instructions for building the example implementation, allowing you to replicate all or parts of this project.

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/critical-cybersecurity-hygiene-patching-enterprise. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at cyberhygiene@nist.gov.

COLLABORATORS

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.