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

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

September 2020

PRELIMINARY DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/building-blocks/patching-enterprise

Executive Summary

WHY WE WROTE THIS GUIDE

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 is collaborating with cybersecurity technology providers to explore approaches for improving enterprise patching practices for general information technology (IT) systems. The guide will include both process and tool usage improvements.

CHALLENGE

There are a few root causes for many data breaches, malware infections, 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 address those root causes. That prevents many incidents from occurring, lowers the potential impact of incidents that do occur, and increases the cost to the attacker. In other words, security hygiene practices make it harder for attackers to succeed and reduce the damage they can cause.

Unfortunately, security hygiene is easier said than done. Despite widespread recognition that (a) patching is effective and (b) attackers regularly exploit unpatched software, many organizations 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. However, delaying patch deployment gives attackers a larger window of opportunity.

Many organizations lack tools to help them measure and assess the effectiveness and timeliness of their patching efforts. They also struggle to prioritize patches, test patches before deployment, and adhere to policies for how quickly patches are applied in different situations.

SOLUTION

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

Once available, the full practice guide can help your organization improve its security and reduce the likelihood of privacy breaches with sensitive personal information by:

- overcoming common obstacles involving enterprise patching for general IT systems
- achieving a comprehensive security hygiene program based on existing standards, guidance, and publications

- enhancing its recovery from incidents that occur and minimizing the impact of incidents on the organization and its constituents

The guide will provide:

- a detailed example solution and capabilities that address risk and security controls
- a demonstration of the approach for operating systems, applications, and firmware using commercially available products
- "how-to" instructions for implementers and security engineers on integrating and configuring the example solution into their organization's enterprise, in a manner that achieves security goals with minimum impact on operational efficiency and expense

The NCCoE is assembling existing commercial and open source tools to aid with the most challenging aspects of patching. The NCCoE is building 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*.

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

When completed, this guide will contain four volumes:

- NIST SP 1800-31A: *Executive Summary – why we wrote this guide, the challenge we address, why it could be important to your organization, and our approach to solving this challenge.*
- NIST SP 1800-31B: *Security Risks and Recommended Best Practices – guidance on deploying, securing, maintaining, and using enterprise patch management technologies.*
- NIST SP 1800-31C: *Approach, Architecture, and Security Characteristics – what we built and why, including the risk analysis performed, and the security/privacy control map.*
- NIST SP 1800-31D: *How-To Guides – instructions for building the example implementation, including all the details that would allow one to replicate all or parts of this project.*

SHARE YOUR FEEDBACK

The comment period for the preliminary draft of this volume ends Oct. 9, 2020. Comments may be submitted to cyberhygiene@nist.gov with the Subject "Comments on Patching VolA-PD1". All comments are subject to release under the Freedom of Information Act (FOIA). There will be at least one additional comment period for this volume.

The other volumes of this guide will be released for review and comment on different schedules so that each volume is made available as soon as possible, rather than delaying the release of completed volumes until all other volumes are also completed. You will be able to view or download them at https://www.nccoe.nist.gov/projects/building-blocks/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.

TECHNOLOGY PARTNERS/COLLABORATORS

Organizations 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). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) 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.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

Visit https://www.nccoe.nist.gov
nccoe@nist.gov
301-975-0200