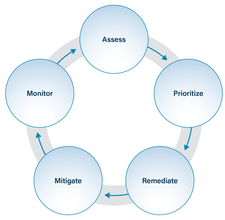
Patching and Vulnerability Management

Patching is the process of applying available software updates to an operating system, application, browser, mobile app, plugin or other type of software. While patches may bring new and useful functionality, patches are also security updates that address known vulnerabilities that could allow cyber threat actors unauthorized access to information systems or networks. While there are some differences, for the purposes of this guide, patching and vulnerability management are synonymous.

Unpatched vulnerabilities remain one of the primary infection vectors observed by the EI-ISAC and our partners. Once patches are publicly announced, information on the associated vulnerabilities they remediate is generally available to anyone, including cyber threat actors. This significantly increases the likelihood that the threat actors will attempt to exploit unpatched systems using information deduced from the patch release.

Software development companies, such as Microsoft and Adobe, regularly release bulk security patches for their products on the second Tuesday of every month, which is known as Patch Tuesday. Other companies release patches on other days of the month, quarterly, or on an ad hoc basis. In the U.S., most publicly known cybersecurity vulnerabilities are cataloged in the National Vulnerability Database (NVD) maintained by NIST. Each vulnerability in the patch is rated based on the associated level of risk, threat, and impact, along with other factors. The NVD frequently asked questions provide a wealth of information on the NVD.

Successful exploitation of unpatched election infrastructure may result in data breaches, malware infections, and website defacements, among other things. Information at risk includes personally identifiable information (PII) and other voter information.



The MS-ISAC regularly disseminates Cybersecurity Advisories, which address critical patches in commercial software commonly used by government agencies and are available to all EI-ISAC members. To subscribe to Cybersecurity Advisories, EI-ISAC members should contact their account manager or complete the subscription form.

Goals

1. Understand the importance of patching (Level 1 maturity)
2. Establish a patching schedules (Level 1 maturity)
3. Establish and execute on a policy for systems that need additional approvals prior to patching (Level 1 maturity)
4. Establish a formal patch management plan leveraging automated tools and aligned with your asset management plan (Level 2 maturity)

Actions

For Patching and Vulnerability Management, the necessary actions vary by maturity as detailed below.

Level 1 Maturity

At the Level 1 maturity, organizations should simply begin patching their systems in a thoughtful and consistent manner.

Not all systems used in elections can be patched immediately. Particularly when patching voting systems, be sure to consider your state's or the U.S. Election Assistance Commission's (EAC) System Certification Process and account for scheduled primary and election day system configuration freezes.

1. Verify that all software used in the office is supported by an active development company. If not, update or replace the software. Only download patches from authoritative sources.
2. Patch all operating systems on a regular timetable.
   - It's usually best to patch your operating systems first, and then move to your software applications. Systems should be set to update by automatically.
   - Network devices also need to receive software updates, but this may require a consultation with IT staff or contractors before it's agreed to patch these devices.
   - Devices and applications will often make patches available via a diagnostic menu or administrative console. Each device or application will be different, and this may require some research.
3. Patch all software applications on a regular timetable.
4. Where complex or mission critical systems are used, test and verify patches before patching production systems.

Level 2 and Level 3 Maturities

Organizations operating at a Level 2 or Level 3 maturity should take additional actions, including:

1. Use automated tools to conduct software patching of your systems.
2. Establish a formal, written plan in place that references the organization's vulnerability management program, as identifying and remediating vulnerabilities goes hand-in-hand with updating software.
   - When creating a patch management program for your office, begin by understanding all the hardware and software assets that you are responsible for by conducting Asset Management. Then implement a conssistent process that:
     - Readily identifies patches as they become available.
     - Prioritizes patches for known vulnerable systems.
     - Downloads patches from authoritative sources.
     - Tests and verifies patches in the operating environment.
     - Applies appropriately tested patches to vulnerable systems.

For more comprehensive recommendations and technical insight on this topic, please see the MS-ISAC's Technical White Paper Timely Patching Reduces System Compromises.

Cost-Effective Tools

- GCA Cybersecurity Toolkit for Elections: Update Your Defenses: A toolbox with links to free tools relevant to this best practice.
- GCA Cybersecurity Toolkit for Elections: Control Access: A toolbox with several links to free tools relevant to this best practice.
- CIS Benchmarks™: Secure configuration guidelines for 100+ technologies, including operating systems, applications, and network devices.
- CIS SecureSuite® Membership: No-cost membership to EI-ISAC members, with access to CIS-CAT Pro Assessor, CIS Build Kits, CIS Benchmarks, and more.
- CIS-CAT® Pro Tool: Scans for proper CIS Benchmark configurations for applications, operating systems, and network devices.
- Itarian: Patch management solution for Windows.
- Opsi: A more complicated solution that can help to manage both Windows and Linux platforms.
- OpenVAS: Free, open-source framework for vulnerability scanning and management.
- Nmap: Famous multipurpose network scanner used by system administrators and hackers across the world to identify which devices are connected to your network.
- U.S. National Vulnerability Database (NVD): Repository of standards based on vulnerability management data.

Learn More

- The MS-ISAC's Technical White Paper Timely Patching Reduces System Compromises
- Apple Auto-update - iOS
- Apple Auto-update - MacOS
- Auto-update Windows
- Auto-update MS Office on macOS
- Auto-update Android

Mapping to CIS Controls and Safeguards

- 2.2: Ensure Authorized Software is Currently Supported
- 7.3: Perform Automated Operating System Patch Management
- 7.4: Perform Automated Application Patch Management

Mapping to CIS Handbook Best Practices

- 43, 44, 76