How to Implement Patching

Patching for Small Healthcare Organizations

HHS 405(d)
Aligning Health Care
Industry Security Approaches

What is patching?

Patching is regularly updating your systems by applying security updates provided by the software or device manufacturer.

Why is it important?

Patching your systems is important because it removes vulnerabilities that can be exploited by attackers.

How will this keep my organization safe?

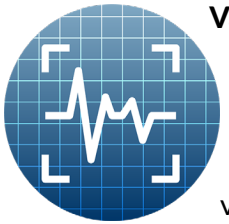
Each patch modifies a software application, rendering it more difficult for hackers to maintain programs that are aligned with the most current version of that software application.

Patching Mitigates:

- Ransomware
- Insider, Accidental, or Intentional Data Loss
- Attacks against connected medical devices that may affect patient safety

Implementation Tips:

Mitigate the most severe vulnerabilities first. Not all vulnerabilities are created equal. Some are easier to exploit than others. The National Vulnerability Database (NVD) has produced the Common Vulnerability Scoring System (CVSS), a standard measurement across all industries that normalizes and ranks the severity of a vulnerability. The goal is to keep the number of new vulnerabilities as low as possible, defined by your organization's level of risk tolerance.



Validate that your patches have been applied to ensure vulnerabilities have been mitigated. It is important to classify and prioritize vulnerabilities that remain after completion of standard patch management practices. Typically, these remaining vulnerabilities are issues that cannot be mitigated with a patch. They may require system configuration changes, code updates, or perhaps even a full blown version upgrade. The process of resolving these vulnerabilities tends to be more time-consuming and complex.

Implement patches that are produced by the vendor community at least monthly. Medical devices should be patched with supported security patches released by the device manufacturers. IT operations should collect these patches, conduct appropriate regression tests to ensure that patches do not negatively impact the business, and schedule patch implementation during routine change windows. This process should be executed and measured using standard IT operations activities.

Remove any end-of-life software that cannot be patched. If your systems are running end-of-life operating systems (OS) or software, associated vulnerabilities should be identified, and steps taken to bring these systems back to a supported state. This may include decommissioning systems that run on unsupported OS, which may require additional investments. Once systems are unsupported, it is usually impossible to apply security patches, potentially increasing the organization's risk posture.

To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. Check out the available resources 405(d) has to offer by visiting our website at 405d.hhs.gov and our social media pages: **@ask405d** *on Facebook, Twitter, LinkedIn and Instagram!*