How to Implement Patching

Patching for Large 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:

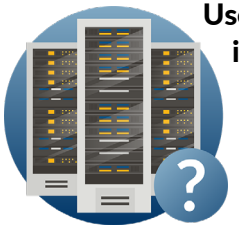
- Ransomware
- Insider, Accidental, or Intentional Data Loss
- Attacks against connected medical devices that may affect patient safety

Implementation Tips:

Create a routine process for patching of medical devices. Enact routine patching as part of preventative maintenance cycles. Medical devices should be patched with supported cybersecurity patches released by the device manufacturers. Given the special sensitivity of the configuration and management of these devices, patching should not take place on these devices unless cleared by the manufacturer. This control, along with whitelisting, can significantly reduce the exploitability of the device.

Develop metrics to monitor patch status. Review the percentage of endpoints that meet all patch requirements each month. The first goal is to achieve a high percentage of success. Secondary goals are to ensure that there are practices to patch endpoints for third-party and operating system-level application vulnerabilities, and to be able to determine the effectiveness of those patches. Without the metric, there might not be checks and balances in place to ensure satisfactory compliance with expectations.

Dispatch field services/desktop support for endpoints that fail to patch. Leaving an endpoint unpatched can result in a breach in which an attacker could exploit the open vulnerability. Deploy resources to areas that are unmanaged to create additional safeguards for the most vulnerable areas of your network.



Use centralized systems to interrogate servers and determine which software updates should be implemented. Automated discovery systems can provide snapshot views of current patching levels for assets. When these snapshots are compared by cybersecurity vulnerability management systems, vulnerabilities due to obsolete software versions will be identified across the network.

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!*