U.S. DEPARTMENT OF
HEALTH AND HUMAN SERVICES
OFFICE FOR
CIVIL RIGHTS

June 2018 OCR Cybersecurity Newsletter

Guidance on Software Vulnerabilities and Patching

Software is the underlying set of instructions that runs computers and other electronic devices. Most software that we use contains "bugs" – mistakes in the software code that negatively affects how the software works. Some of these bugs may introduce security vulnerabilities that, if exploited, could permit hackers unauthorized access to a user's computer or an organization's computer network. Patches are fixes to these bugs to correct how the software operates including closing security vulnerabilities. Patches play an essential role in the software lifecycle as vulnerabilities are regularly discovered in software that can create risks to the confidentiality, integrity, and availability of data. Without patches, such vulnerabilities could not be fixed.

In late 2017, researchers discovered a widespread vulnerability in computer processors that were sold over the previous decade. These vulnerabilities, known as Spectre and Meltdown, allowed malware to bypass data access controls and potentially access sensitive data. The security flaw was present in nearly all processors produced in the last 10 years and affected millions of devices. After the discovery of these defects, vendors scrambled to release patches that addressed this problem. However, testing indicated that a side effect of the patches could be decreased performance in certain computer uses. Testing and understanding the impact of patches can be critical to mitigating the risks patches are designed to address while avoiding or minimizing risks that patches may introduce. HHS published a newsletter discussing such risks in the context of the Spectre and Meltdown vulnerabilities and patches.[1]

Many HIPAA covered entities (CEs) and business associates (BAs) are highly dependent on software for processing and handling of electronic protected health information (ePHI). Under the HIPAA Security Rule, CEs and BAs are required to protect their ePHI, which includes identifying and mitigating vulnerabilities of computer programs and systems that could affect the security of ePHI. Identifying software vulnerabilities and mitigating the associated risks are important activities for CEs and BAs to conduct as part of their security management process and technical evaluations.

Identifying Software Vulnerabilities

HIPAA covered entities (CEs) and business associates (BAs) are required to conduct a risk analysis - an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) they hold.[2] Following a risk

[1] https://content.govdelivery.com/attachments/USDHSCIKR/2018/01/05/file_attachments/939003/HCCIC-2018-001-Spectre-Meltdown-3.pdf.

[2] *See* 45 C.F.R. § 164.308(a)(1)(ii)(A).

analysis, CEs and BAs must implement measures that reduce these risks and vulnerabilities to a reasonable and appropriate level.[3] The scope of the risk analysis and risk management processes encompasses the potential risks and vulnerabilities to all ePHI that an organization creates, receives, maintains, or transmits.

This includes identifying and mitigating risks and vulnerabilities that unpatched software poses to an organization's ePHI. Mitigation activities could include installing patches if patches are available and patching is reasonable and appropriate. In situations where patches are not available (e.g., obsolete or unsupported software) or testing or other concerns weigh against patching as a mitigation solution, entities should implement reasonable compensating controls to reduce the risk of identified vulnerabilities to a reasonable and appropriate level (e.g., restricting network access or disabling network services to reduce vulnerabilities that could be exploited via network access). Security vulnerabilities may be present in many types of software including databases, electronic health records (EHRs), operating systems, email, applets such as Java and Adobe Flash, and device firmware. Each type of program will have its own unique set of vulnerabilities and challenges for patching, but identifying and mitigating the risks unpatched software poses to ePHI is important to ensure the protection of ePHI and in fulfilling HIPAA requirements. Including operating systems, applications, device firmware and other software, along with the versions currently in use, as part of an organization's inventory can aid in determining what systems and applications should be part of an organization's patch management process.

Identifying risks and vulnerabilities in software is no easy task. Today's threat landscape changes rapidly and organizations must be vigilant. One helpful source is the United States Computer Emergency Readiness Team (US-CERT). This organization collects and publishes information on cybersecurity threats for stakeholders in government and industry. OCR's February 2017 cybersecurity newsletter included information on using US-CERT bulletins to help identify vulnerabilities.[4] In addition to following publications, there are a variety of tools that can help CEs and BAs keep their software updated with the latest patches. Vulnerability scanners are software tools used to test systems and networks for known vulnerabilities including identifying outdated or unsupported software. Oftentimes, when threat and vulnerability data is available publically, malicious actors specifically seek out unpatched vulnerabilities on a system to exploit. This means that the timely implementation of patches is an important part of the risk management process.

Patching Software

Patches can be applied to software and firmware on all types of devices – phones, computers, servers, routers, and more. Installing vendor recommended patches is typically a routine process. However, organizations should be prepared in the event that issues arise as a result of applying patches. Computer programs are often interconnected and dependent on the functionality and output of other programs. When certain changes are made, including the installation of a patch, programs dependent on the changed application may not perform as expected because settings or data are affected. This is why in complex environments, patch management plays a crucial role in the safe and correct implementation of these changes. Patch management is the process of "identifying, acquiring, installing and verifying patches for products and systems."[5] This ensures that patches are correctly and safely applied so that

[3] *Id.*
[4] https://www.hhs.gov/sites/default/files/february-2017-ocr-cyber-awareness-newsletter.pdf.
[5] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf.

adverse effects are minimized. Each organization is different and has unique systems, challenges, and needs for this process.

Patches for identified vulnerabilities should be applied, as appropriate, in accordance with an organization's security management process. Each type of program will have its own unique set of vulnerabilities and challenges for patching, but the identification and mitigation of risks associated with unpatched software is important to ensure the protection of ePHI. The following are some common steps to include in effective patch management as part of a security management program:

- *Evaluation*: Evaluate patches to determine if they apply to your software/systems.
- *Patch Testing*: When possible, test patches on an isolated system to determine if there are any unforeseen or unwanted side effects, such as applications not functioning properly or system instability.
- *Approval*: Once patches have been evaluated and tested, approve them for deployment.
- *Deployment*: Following approval, patches can be scheduled to be installed on live or production systems.
- *Verification and Testing*: After deploying the patches, continue to test and audit systems to ensure that the patches were applied correctly and that there are no unforeseen side effects.

Due to the complexity of some systems, installing a patch or collection of patches can be a major undertaking. System modifications that affect the security of ePHI may trigger an entity's HIPAA obligation to conduct an evaluation to ensure that ePHI remains protected following environmental or operational changes[6]. The purpose of this evaluation is to establish a process to review and maintain reasonable and appropriate security measures. Installing patches can introduce a variety of changes to a system - technicians may disable security features in order to access certain services or unanticipated bugs or stability issues may result from an update. An evaluation can help identify new vulnerabilities that may have resulted from these changes. Undiscovered bugs or vulnerabilities are unpleasant surprises that could be exploited and may lead to beaches of PHI.

Additional Resources

United States Computer Emergency Readiness Team: https://www.us-cert.gov/

HIPAA Administrative Safeguards:
https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf?language=es

Meltdown and Spectre:
https://content.govdelivery.com/attachments/USDHSCIKR/2018/01/05/file_attachments/939003/HCCIC-2018-001-Spectre-Meltdown-3.pdf

**This newsletter should not be construed as a final agency action and is not intended to, does not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter civil or criminal.*

[6] *See* 45 C.F.R. § 164.308(a)(8).