Top 11 PCI DSS 3.0 Changes That Will Affect Your Application Security Program

October 2015

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard. It is intended to reduce credit card fraud by ensuring that organizations that are handling branded credit cards protect user data from exposure. The standard has undergone several changes over the past few years; the most recent version is 3.1, which is active until December 31, 2017. This version has a significant impact on the way organizations ensure application security.

PCI DSS version 3.1 addresses several ongoing problems, including a lack of education and awareness surrounding the standard, weak passwords and authentication, third-party security challenges, and inconsistency in assessments.

These changes will increase security for sensitive information, but they could also increase your workload. In this whitepaper, we discuss the top ten ways your web application security will be affected and the steps you can take to ensure that you are compliant with the new standard, including best practices and practical steps for implementation.

Change #1: Coding Practices

Requirement 6.5

Address common coding vulnerabilities in the software-development processes.

How Does This Affect You?
Prior to version 3.0, the standard did not specifically outline how vulnerabilities should be addressed throughout the entire lifecycle; Requirement 6.5 now explicitly calls for examination of the software development lifecycle (SDLC) to ensure vulnerabilities are not introduced at the time of coding. It states that application developers should be properly trained to identify and resolve issues related to common coding vulnerabilities, and should be knowledgeable about secure coding guidelines. Training can be provided in-house or by third parties and should be applicable to the technologies used.

Recommended Activity
Implement a secure coding training program that includes Computer Based Training (CBT) and/or live training.

Change #2: Risk Assessments

Requirement 12.2 (Previously 12.1.12)

Implement annual assessments at a minimum, and assess when significant changes are made.

How Does This Affect You?
This requirement has received the most attention, since it requires that assessments be performed annually at a minimum. More importantly, it requires assessments to be redone any time there is a significant change to your applications. If you are not currently performing assessments on a regular basis, this requirement may increase the number of assessments you need to perform. In today's agile coding environment, changes are frequent and assessments should be performed just as regularly.

Recommended Activity
Establish a security program that performs assessments each time there are major changes in applications. The best practice is to perform continuous monitoring.

Change #3: Cryptographic Protocols

Requirement 2.2.3 / 2.3 / 4.1 / 4.1.1

SSL and early versions TLS are no longer considered secure.

How Does This Affect You?
As a response to many of the recent network layer vulnerability exploitations, PCI DSS has implemented changes that make applications using SSL and early versions of TLS no longer PCI compliant. Your web applications should not accept SSL or older versions of TLS. Also, it is not sufficient to just support newer version of TLS, you also have to disallow older versions in order to remain compliant.

Recommended Activity
We recommend you scan for SSL and outdated TLS versions being used by your applications. Additionally, configure your web applications to only accept connections using TLS 1.1 or 1.2 versions.

Change #4: Inventory

Requirement 2.4

Maintain a current list of all system components.

How Does This Affect You?
Historically, compliance with PCI DSS required maintaining a current list of all systems and their components. This requirement now goes further to say that you also need to understand what each component is doing in order to properly define the scope of the environment for implementing PCI DSS controls. In large environments, taking inventory is often labor intensive, time-consuming and complex. To alleviate some of that manual investment, you will want to automate as much of this as possible.

Recommended Activity
We recommend you perform quarterly discovery of environments. PCI doesn't state that you must do this yourself; you can have a third party assist with this task as long as you are the overall owner and arbiter of the resulting list.

Change #5: Attestation

Requirement 12.8.5

Maintain detailed documentation about PCI DSS requirements managed by vendors and by the organization itself.

How Does This Affect You?
In prior versions of the standard, you were not required to know and document what party is handling which activities related to the requirements. The updated requirement adds new, time-consuming, activities.

Recommended Activity
We highly recommend that for activities being handled by third parties, you simply request that the third parties attest to the activities they're doing and include that attestation in your matrix. When a third party tests for requirements, that third party should provide attestation on your behalf.

Change #6: Vulnerability Classes

Requirement 6.5.1 – 6.5.10

Requirements 6.5.1 – 6.5.10 now apply to all internal as well as external applications.

How Does This Affect You?
In the past, hackers would occasionally exploit internal applications that contain cardholder data. Although those applications were already within the scope of the requirements, the PCI Security Standards Council has clarified and expanded the requirement to state that all classes of vulnerabilities—6.5.1 through 6.5.10—are now within scope. The vulnerabilities at issue are injection flaws, particularly SQL injection and OS command injection. Other vulnerabilities include buffer overflows into your cryptographic storage and your communication, improper error handling, and cross-site scripting.

Recommended Activity
The recommended activity here is relatively straightforward: make sure your application security program covers all of the mentioned vulnerabilities, and covers them for all internal systems. The work you do in the inventory process (Change #3), should make it easier to understand the scope for this requirement.

Change #7: Insecure Cryptographic Storage

Requirement 6.5.3

Prevent cryptographic flaws. Use strong cryptographic algorithms and keys.

How Does This Affect You?
This requirement covers a class of vulnerabilities relating to the insecure storage of sensitive data. All vulnerabilities in this class relate to ensuring your data is encrypted when and where it needs to be. Dynamic testing alone will not suffice for finding cryptographic flaws.

Recommended Activity
Examine software development policies and procedures and implement static analysis testing. That will include ensuring the encryption of the correct data, ensuring you have proper key storage and management, and ensuring that you are not using known bad algorithms.

Change #8: Broken Authentication and Session Management

Requirement 6.5.10

Authentication and session management includes all aspects of handling user authentication and managing active sessions.

How Does This Affect You?
Authentication is a critical aspect of the overall process; however, it's not enough simply to have strong authentication mechanisms, since they could be compromised if credential management is flawed. Credential management functions might include password-change, forget-my-password, remember-my-password, account update and similar functions. Note that 6.5.10 was a best practice until June 30, 2015, after which it became a requirement.

Recommended Activity
Consider using a framework that enforces proper session management.

Change #9: Review Custom Code

Requirement 6.3.2

Review custom code prior to the release to production.

How Does This Affect You?
Security vulnerabilities in custom code are commonly exploited and can be difficult to defend against with, for example, a web application firewall. Vulnerable code is much more difficult and expensive to address after it's been deployed into production environments. Requirement 6.3.2 now calls for reviewing custom code before deployment, underscoring the fact that the standards council is now focusing on the overall development lifecycle and expanding its guidance to include testing and review of custom code during preproduction.

Recommended Activity
Implement a process for code review that includes secure coding practices. Automated code reviews should be paired with manual review as well.

Note that the new standard states that individuals other than the originating code author must review code changes. Therefore, if you purchase off-the-shelf software and make changes to it, this requirement applies as if you'd written the entire application from scratch: the entire application would have to be reviewed by another individual, who had written neither the original application nor your custom changes.

Change #10: Development & Test User Accounts

Requirement 6.3.1

Remove development, test and/or custom application accounts, user IDs, and passwords.

How Does This Affect You?
Often developers leave development, test, and/or custom application accounts, user IDs, and passwords in software so that testing can be done in live environments, especially in a continuous integration environment. The new requirement now includes pre-production and custom application accounts in the definition of "sensitive data" to ensure this data does not carry into production environments. While in the past it may have been sufficient to ensure that such accounts, IDs, or passwords were being stored securely, they must now be removed completely. Although this sensitive data may be difficult for malicious hackers to find, there are means by which they could discover and leverage it.

Recommended Activity
Expand the scope of your assessment efforts to include hard-coded authentication and passwords not found during dynamic testing.

#11: PCI Compliance Is an Ongoing Activity

Requirement 1 – 12!

All PCI requirements now call for maintaining a regular process to ensure compliance.

How Does This Affect You?
You will now see the word "maintaining" throughout the new requirements, including process maintenance. The Council is making the point that compliance is an ongoing activity, not simply a task to perform in order to pass an audit. This is a very important change, and will have a tremendous impact on the way assessments are performed. While many organizations have looked at PCI DSS compliance as an annual requirement, it is now required to be an ongoing process. Failure to comply may lead to data exploits, which can result in hefty fines and negative impact to the brand and customer satisfaction.

Recommended Activity
Continuously monitor your applications for change and new vulnerabilities. Remediate vulnerabilities as they are found. Test through all stages of the development lifecycle.

Reaching the Overall Objective of Version 3.0

The overarching objective of the 3.0 standard is to ensure that organizations reach and maintain operational compliance with all PCI DSS requirements 24 hours a day, 365 days a year, year after year. We encourage you to keep that goal in mind when you introduce any new process or controls intended to satisfy the requirements.

WhiteHat SECURITY

About WhiteHat Security
Founded in 2001 and headquartered in Santa Clara, California, WhiteHat Security is the leader in application security, enabling businesses to protect critical data, ensure compliance, and manage risk. WhiteHat is different because we approach application security through the eyes of the attacker. Through a combination of technology, more than a decade of intelligence metrics, and the judgment of real people, WhiteHat Security provides complete web security at a scale and accuracy unmatched in the industry. WhiteHat Sentinel, the company's flagship product line, currently manages tens of thousands of websites – including sites in highly regulated industries, such as top e-commerce, financial services, and healthcare companies. For more information on WhiteHat Security, please visit www.whitehatsec.com.

WhiteHat Security, Inc. | 3970 Freedom Circle | Santa Clara, CA 95054 | 1.408.343.8300 | www.whitehatsec.com