

PCI DSS v4.0

# Vulnerability Scanning

written by  
Jeff Man  
Security Evangelist  
Risk, Security, and Privacy  
Online Business Systems

The new PCI DSS v4.0 requires many significant changes to your organization's data security program. One change that is sure to be a challenge involves the requirement to perform authenticated scans to satisfy internal vulnerability scanning. While most organizations strive for "less is more" when it comes to scan findings, this new requirement is sure to cause some push back. In this eBook we explore the history and evolution of vulnerability scans and how the new changes will impact PCI security programs.

PCI PAST

YOU ARE HERE

ROAD AHEAD

online



A hand is shown holding a red pushpin, which is pinned to a technical drawing on a grid background. The drawing consists of various geometric shapes and lines, including a prominent circle and several rectangular outlines. The background is a light blue color with a subtle grid pattern. The pushpin is positioned in the upper right quadrant of the page, with its sharp point resting on the grid. The hand holding the pushpin is partially visible at the top of the frame. The overall scene suggests a focus on precision and technical details.

## Section Guide

Introduction .....	3
Background .....	4
PCI DSS v4.0 – The Details .....	8
Authenticated (Credentialed) Vulnerability Scanning .....	10
Observations .....	12
Recommendations .....	14
References and Additional Reading .....	16

---

One of the most significant changes introduced in PCI DSS v4.0 involves the documented approach for performing internal vulnerability scans. The internal vulnerability scanning requirement (now 11.3.1) contains more explicit details intended to provide clarification of the requirement:

- 📍 Perform scans at least once every three months.  
*Formerly “four quarterly vulnerability scans”*
- 📍 High-risk and critical vulnerabilities (per the entity’s vulnerability risk rankings defined in Requirement 6.3.1) are resolved.  
*Formerly “high-risk vulnerabilities”; formerly “addressed”*
- 📍 Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved.  
*Formerly “high-risk vulnerabilities”*
- 📍 Scan tool is kept up to date with latest vulnerability information.
- 📍 Scans are performed by qualified personnel and organizational independence of the tester exists.

However, the **big changes** are found in the following sub-requirements:

**11.3.1.1** All other applicable vulnerabilities (those not ranked as high-risk or critical (per the entity’s vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows:

- 📍 Addressed based on the risk defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.
- 📍 Rescans are conducted as needed.

**11.3.1.2** Internal vulnerability scans are performed via authenticated scanning as follows:

- 📍 Systems that are unable to accept credentials for authenticated scanning are documented.
- 📍 With sufficient privileges, for those systems that accept credentials for scanning.
- 📍 If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with Requirement 8.2.2.

To summarize, entities need to perform authenticated/credentialed scanning, considered to be more thorough, which will yield more accurate findings (emphasis on “more”) and they will also need to address ALL the findings not just “high-risk” and “critical” findings. The good news is that “this requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.”

The intent of this article is to provide historical context, explanation, and best practice recommendations as entities plan for changes to their security testing programs to meet the new vulnerability scanning requirements found in PCI DSS v4.0.





PCI PAST

# BACKGROUND



## PCI Past

Since the initial release of the Payment Card Industry Data Security Standard (PCI DSS) in December 2004 there has been a requirement to conduct periodic network vulnerability scans (both internal and external) as part of a continuous process of monitoring and testing your network (Requirement 11). Curiously, the capability to perform an authenticated/credentialed scan has been around since roughly the same time frame.

Regularly Monitor and Test Networks	
Requirements	Testing Procedures
<p><b>11.2</b> Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (e.g., new system component installations, changes in network topology, firewall rule modifications, product upgrades).</p> <p><i>Note that external vulnerability scans must be performed by a scan vendor qualified by the payment card industry.</i></p>	<p><b>11.2.a</b> Inspect output from the most recent four quarters of network, host and application vulnerability scans to verify that periodic security testing of the devices within the cardholder environment occurs. Confirm the scan process includes rescans until "clean" results are obtained.</p> <p><b>11.2.b</b> To verify that external scanning is occurring on a quarterly basis in accordance with the PCI Security Scanning Procedures, inspect output from the four most recent quarters of external vulnerability scans to verify the following:</p> <ul style="list-style-type: none"><li>• Four quarterly scans occurred in the most recent 12-month period.</li><li>• The results of each scan satisfy the PCI Security Scanning Procedures (e.g., no urgent, critical, or high vulnerabilities).</li><li>• The scans were completed by a vendor approved to perform the PCI Security Scanning Procedures.</li></ul>

Figure 1: PCI DSS v1.0 release December 2004

Entities who were subject to this requirement immediately questioned the compliance criteria for internal scans; there was guidance for the external scans (in fact, there is a separate program that takes care of that) but what about internal scanning? Essentially, what constitutes a "clean" result for a scan? The first official guidance provided by the PCI Security Standards Council was found in the release of PCI DSS v2.0 in October 2010, although the term "clean" was replaced by "passing" in terms of scanning results.

The definition of what constitutes “passing” results was provided for both internal and external vulnerability scans. For internal scans, the threshold was “all ‘High’ vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved” (more on Req. 6.2 further down). For external scans, the threshold was different: scan results must “satisfy the ASV Program Guide requirements”. For example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures.

## What is CVSS?

CVSS stands for Common Vulnerability Scoring System and is an industry-accepted scoring criteria that considers such things as the complexity of the attack that could exploit the vulnerability, whether attacks already exist “in the wild”, and other environmental factors such as network topology, defense-in-depth, or location of the vulnerable system in relation to open, untrusted networks such as the Internet.



### *Approved Scanning Vendors*

The ASV Program Guide, which was first published in March 2010, actually provided a fairly detailed breakdown of Pass/Fail based on the CVSS scoring (see Figure 2, next page). External scanning, because they are required to be performed by an Approved Scanning Vendor (ASV) are fairly well regulated and understood. You have a scan performed by an ASV that issues a report that clearly indicates “PASS” or “FAIL”. That’s fairly straightforward and easy to determine if the entity is adhering to the corresponding PCI DSS requirement.

The determination of whether internal vulnerability scans are adhering to the requirement is not as straightforward. What does it mean to: 1) resolve all “high” vulnerabilities, and 2) why the reference to requirement 6.2?



**Table 2: Vulnerability Severity Levels Based on the NVD and CVSS Scoring**

CVSS Score	Severity Level	Scan Results	Guidance
7.0 through 10.0	High Severity	Fail	To achieve a passing scan, these vulnerabilities must be corrected and the environment must be re-scanned after the corrections (with a report that shows a passing scan). Organizations should take a risk-based approach to correct these types of vulnerabilities, starting with the most critical ones (rated 10.0), then those rated 9, followed by those rated 8.7, etc., until all vulnerabilities rated 4.0 through 10.0 are corrected.
4.0 through 6.9	Medium Severity	Fail	
0.0 through 3.9	Low Severity	Pass	While passing scan results can be achieved with vulnerabilities rated 0.0 through 3.9, organizations are encouraged, but not required, to correct these vulnerabilities.

*Figure 2: Passing Criteria from ASV Program Guide, March 2010*

The answer to the first question involves doing something about the vulnerabilities discovered that, based on their CVSS score, make you most vulnerable to attack or compromise. The blanket term “resolve” was intended to encompass all the ways you could make the vulnerability go away – typically through configuration changes, upgrading to a newer version, and/or applying patches.

There is another way to approach resolving vulnerabilities and that is what the second question [the inclusion of 6.2 in the requirement] is all about. PCI DSS 6.2 states, “Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.” The implicit meaning of this reference is that you are required (allowed) to address the vulnerabilities in your scan findings by YOUR OWN risk scores – not merely the scores provided by whatever scan engine you use. The major scan engine vendors call this process “vulnerability prioritization” or “risk-based vulnerability management”.

Subsequent revisions of the PCI DSS (v3.0 in 2013 through v3.2.1 in 2018) contained no material changes to the internal vulnerability scanning requirements and that brings us up-to-date until the new changes introduced in the v4.0 release are in full effect.



An aerial photograph of a winding asphalt road on a hillside. The road curves through a landscape with green trees and dry, brownish brush. The lighting suggests late afternoon or early morning. A small blue car is visible on the road in the lower left. The text 'YOU ARE HERE' is overlaid on an orange bar, and 'THE DETAILS' is overlaid in large white letters.

YOU ARE HERE

# THE DETAILS



## The Details

Let's summarize the new aspects of the vulnerability scanning requirements (**11.3.1 -11.3.1.3**) and provide some explanation and clarification based on my experiences as a QSA.



### Quarterly Scanning Clarified

At least once every three months – This attempts to provide clarity to those entities that believe quarterly scanning could be “once within a quarter” meaning they could scan in January for Q1 and June for Q2 and still be adhering to the requirement. Nope.



### High-Risk and Critical Vulnerabilities

High-risk and critical vulnerabilities are resolved – The implied meaning of the criteria was always “high-risk and higher” but sometimes it's better to put it in writing to help clarify meaning.



### Rescans

Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved – Added the “and critical” to be consistent with the initial scan. Bottom line – fix it!



### Scan Tool Update

Scan tool is kept up to date with latest vulnerability information – This is an apparent nod to the scan vendors these days that tout themselves as vulnerability management solutions and want you to rely on scanning for the identification of vulnerabilities (per PCI DSS v4.0 rfmt 6.3.1). The more direct interpretation is that updated scan engines will find the newest vulnerabilities.



### Applicable Vulnerabilities Managed

All other applicable vulnerabilities are managed – This means you can no longer ignore informational, low, or medium risk findings. You don't necessarily need to resolve them, but you do need to explicitly acknowledge they are there, have a potential impact, and demonstrate that you have considered the overall risk of the vulnerability remaining in your environment.



### Authenticated Scanning

Internal vulnerability scans are performed via authenticated scanning – Wait, what? That's right, Your scan that used to have a handful of low-risk findings is about to contain hundreds, maybe thousands of findings that you will have to address.

The requirement for authenticated scanning is the biggest change and deserves a closer look.

## Authenticated (Credentialed) Vulnerability Scanning

The ability for a vulnerability scan to remotely login to a system using credentials has existed in the major scan engines since about the time the first PCI DSS was published back in 2004. The rationale for performing a scan by actually logging into the target system is pretty simple – you get better, more accurate results because you can actually see what’s running on the target system.

Remember, the way that vulnerability scanners ‘detect’ vulnerabilities is by querying a target on multiple TCP/IP ports and seeing what type of response is given. Vulnerabilities are discovered based on the services that respond to queries and how they respond. Often the vulnerabilities are guesses based on assumptions – “if you’re running the XYZ service there are the following issues with XYZ service”. The service may or may not be running, it may be running a version that has already been patched or fixed, or it may in fact be vulnerable. These educated guesses sometimes result in what is called a “false positive” and those responsible for fixing the problems have to provide evidence that proves the false positive – which is often a very tedious exercise.

The promise of an authenticated scan is that false-positives are greatly reduced because the guessing/guilt-by-association element of scan findings is eliminated. Authenticated scans also yield more findings because they are getting a truer snapshot of the targeted system. A Qualys blog on “Unified Vulnerability View of Unauthenticated and Agent Scans” provided some side-by-side results:



Figure 3: Unauthenticated vs. Authenticated Scan Results

What is even more compelling in terms of using authenticated scans is how they reveal more severe vulnerabilities that expose the entity to compromise.

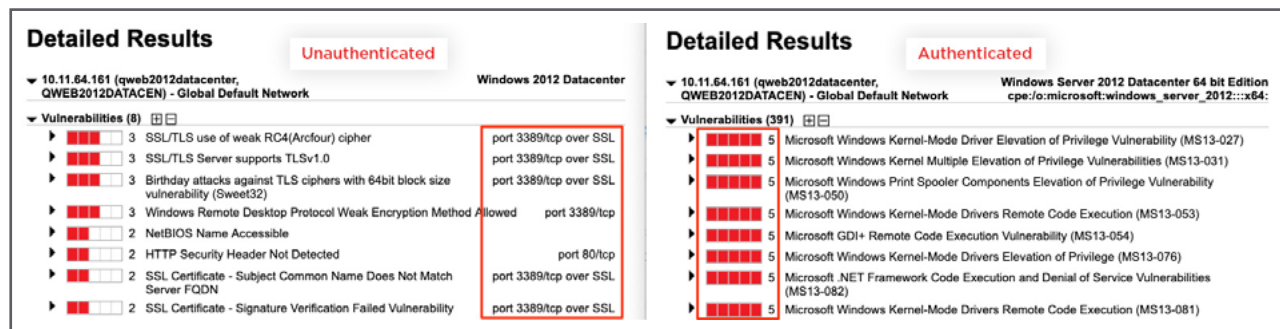


Figure 4: Detailed Findings of Both Scans




Other scan vendors have similar studies and examples (see the reference 'Additional Reading' section at the end of this article).

The ability to detect more accurate vulnerabilities, uncover more critical findings, and more comprehensive results seems like a no-brainer. Yet, this capability is not universally accepted or practiced, particularly by entities that are subject to PCI DSS compliance. The paradox is that too many companies want to find fewer results – so they have less cleanup and remediation work to do – rather than find more accurate and impactful results.

This is why this new requirement is expected to be so disruptive and why the Council is giving entities nearly three years to put it fully in place.

## EASIER SAID THAN DONE

A close-up photograph of a hand reaching out from a car window. The hand is positioned as if gesturing or waving. The background is a soft, out-of-focus sunset with warm orange and yellow tones. The car's side mirror and door handle are visible in the foreground.

"Vulnerability scanning has evolved significantly over the past few decades. But the key goal remains the same, which is to accurately identify vulnerabilities, assess the risk, prioritize them, and finally remediate them before they get exploited by an attacker.

Therein lies the challenge. It is easier said than done. There are multiple ways to scan an asset, for example credentialed vs. uncredentialed scans or agent based vs. agentless."

– Spencer Brown, Security Solutions Architect, Qualys





SECURITY GOALS

# OBSERVATIONS



## Observations

Now is a good time to remind the reader that PCI DSS compliance is ultimately trying to hold entities to an industry best-practice level of implementation of a security program that prevents certain breach attempts but also detects malicious activities that lead to breaches and compromise.

PCI Data Security Standard – High Level Overview		
<b>Build and maintain a Secure Network and Systems</b>	1.	Install and maintain network security controls to protect the cardholder data environment.
	2.	Apply secure configurations to all system components.
<b>Protect Cardholder Data</b>	3.	Protect stored cardholder data.
	4.	Protect cardholder data with strong cryptography during transmission.
<b>Maintain a Vulnerability Management Program</b>	5.	Protect all systems and networks from malicious software.
	6.	Develop and maintain secure systems and software.
<b>Implement Strong Access Control Measures</b>	7.	Restrict access to system components and cardholder data by business need to know.
	8.	Identify users and authenticate access to system components.
	9.	Restrict physical access to cardholder data.
<b>Regularly Monitor and Test Networks</b>	10.	Log and monitor all access to system components and cardholder data.
	11.	Test security of systems and networks regularly.
<b>Maintain an Information Security Policy</b>	12.	Support information security with organizational policies and programs.

Figure 5: Primary Security Goals of PCI

It's important to remember that the PCI DSS is organized according to six primary goals that are reflected in twelve major requirements. Note that there is a primary goal entitled "Maintain a Vulnerability Management Program" but the requirements for vulnerability scanning is found in Requirement 11 "Test security of systems and networks regularly" which is part of the primary goal to "Regularly Monitor and Test Networks". Consider that the major scan engine vendors universally call their products "vulnerability management" solutions yet PCI DSS considers vulnerability scanning to be a function of regularly testing and monitoring the security of your systems and network.

There is certainly a connection between the two – especially since the ranking of internal scan findings is required to be based on an internal risk ranking system (Requirement 6.2.1) – which is an integral part of your vulnerability management program. The major difference between the implied expectation of PCI DSS and the way the industry views scan engines is that PCI expects a vulnerability scan to be executed as a check or safety net to see how well all of your security tools and processes are working in order to maintain secure operations while the scan engines expect you to run the scan as a baseline or starting point to determine what is insecure. Very often the resolution of findings – namely patching, reconfiguration, or updating to a newer version – are all required to be performed by PCI DSS prior to executing a scan.

The new requirement to use authenticated scanning further reinforces this idea of continuous testing and monitoring by providing more detailed information that reflects efficacy of such elements as network segmentation/access controls (Requirement 1), secure hardening and configuration requirements (Requirement 2), patching, version control, change control (Requirement 6), or user account information (Requirement 8).



A photograph of a dirt road that splits into two paths, leading into a field of tall, golden-brown grass. The sky is filled with dramatic, orange and red clouds, suggesting a sunset or sunrise. The sun is visible on the horizon, creating a bright glow. The overall mood is contemplative and forward-looking.

THE ROAD AHEAD

# RECOMMENDATIONS



## Recommendations

Of course, you will want to try an authenticated scan and scan early and often to determine how many more findings are discovered and remember that ALL of the findings are now either to be mitigated or addressed according to the 'new rules' found in the PCI DSS v4.0.

If you're not doing so already, pay close attention to the requirement (new: 6.3.1/old: 6.2.1) for developing a risk ranking (remember this has been required since PCI DSS v2.0). There is new guidance for this requirement that states:

***“Note: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.*”**

***Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a “high risk” to the environment. In addition to the risk ranking, vulnerabilities may be considered “critical” if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.”***

While conducting the research for this article, I spoke to colleagues at the “big three” vendors – Qualys, Rapid7, and Tenable. Besides the question of “which type of scan is better”, I asked the question, “does each type of scan provide the same results?” They all acknowledged that there are some conditions that can only be effectively tested from an external viewpoint. Meaning that while an authenticated scan gives you better results of what is/isn't a vulnerability on the targeted system it doesn't report all the valid findings of an unauthenticated scan. Everyone agreed that the best option is to perform both methods of scanning.

The biggest hurdle for those entities that take a minimalist approach to scanning, security, and PCI in general will be to address all the new vulnerabilities that are about to be discovered in their environments. There are those entities that properly embrace the security goals of PCI DSS already so they should have fewer issues and surprises; they might already be taking advantage of authenticated scans.

The RSP practice at Online Business Systems is always available to help evaluate the results of scans and to help with security architecture and strategies to promote “passing” scans in the days to come.

**Happy hunting!**

## REFERENCES & ADDITIONAL READING

The following is a list of the linked resources mentioned above, reprinted here for easy reference.

PCI DSS v4.0	<a href="https://www.pcisecuritystandards.org/document_library">https://www.pcisecuritystandards.org/document_library</a>
PCI SSC FAQs	<a href="https://www.pcisecuritystandards.org/faqs">https://www.pcisecuritystandards.org/faqs</a>
Summary of Changes PCI DSS v4_0.pdf	<a href="https://www.pcisecuritystandards.org/document_library">https://www.pcisecuritystandards.org/document_library</a>
PCI DSS v4.0 Hitchhiker's Guide to v4.0.pdf	<a href="https://info.obsglobal.com/hubfs/PCI%20DSS%20v4.0%20-%20Hitch-Hikers%20Guide%20to%20v4.0%20-%20eBook.pdf">https://info.obsglobal.com/hubfs/PCI%20DSS%20v4.0%20-%20Hitch-Hikers%20Guide%20to%20v4.0%20-%20eBook.pdf</a>

Qualys – Unified Vulnerability View of Unauthenticated and Agent Scans	<a href="https://blog.qualys.com/product-tech/2021/01/21/unified-vulnerability-view-of-unauthenticated-and-agent-scans">https://blog.qualys.com/product-tech/2021/01/21/unified-vulnerability-view-of-unauthenticated-and-agent-scans</a>
--	---

Rapid7 - Authentication on Unix and related targets: best practices	<a href="https://docs.rapid7.com/insightvm/authentication-on-unix-and-related-targets-best-practices/">https://docs.rapid7.com/insightvm/authentication-on-unix-and-related-targets-best-practices/</a>
---	---

Rapid7 - Authentication on Windows: best practices	<a href="https://docs.rapid7.com/insightvm/authentication-on-windows-best-practices/">https://docs.rapid7.com/insightvm/authentication-on-windows-best-practices/</a>
--	---

Tenable - Credentialed Checks on Windows	<a href="https://docs.tenable.com/nessus/Content/CredentialedChecksOnWindows.htm">https://docs.tenable.com/nessus/Content/CredentialedChecksOnWindows.htm</a>
--	---

Tenable - Credentialed Checks on Linux	<a href="https://docs.tenable.com/nessus/Content/CredentialedChecksOnLinux.htm">https://docs.tenable.com/nessus/Content/CredentialedChecksOnLinux.htm</a>
--	---

---

# online

Founded in 1986, Online Business Systems is a Digital Transformation and Cybersecurity consultancy. We help enterprise Clients by designing improved business processes enabled with secure information systems. Our unsurpassed delivery, our people, and the Online culture of loyalty, trust and commitment to mutual success set us apart.