PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) V4.0

Authenticated Scanning for Internal Quarterly Scans

INTERNAL VULNERABILITY SCANS ARE PERFORMED USING AUTHENTICATED ACCESS

The Payment Card Industry Data Security Standards (PCI DSS) V4.0 have enhanced requirements for internal vulnerability scans, requiring authenticated scanning. Authenticated scans allow for a deeper dive into the systems and can identify more vulnerabilities than an unauthenticated scan is able to.

What is the difference between authenticated and unauthenticated scans?

Authenticated: The scanning tool accesses the system with approved credentials. The authorized access allows the scanning tool to identify vulnerabilities based on the access permissions of the account.

Unauthenticated: The scanning tool does not have access to the system, and the scanning results are similar to a scan without permissions, or from another perspective, a scan from an outside viewpoint.

The authenticated scan requirement pertains to internal vulnerability scanning, and the new requirement intends to obtain in-depth results and details from the scanning tool.

The results should include information regarding installed libraries, program versions, configurations, software operating on the systems, and insight into the possible risks to a system when using a scanning tool with authentication enabled.

The authenticated scanning tools can be either host-based or network-based.

The account used by the scanning tool needs sufficient privileges to access system resources to gather the information described above. The goal is to determine if possible vulnerabilities exist. The privileged account is also assessed in PCI DSS requirements 7 and 8, as the account is considered a highly privileged account.

This requirement does not apply to system components that cannot obtain credentials for scanning. Examples of systems that may not accept credentials for scanning include some network and security appliances, mainframes, third-party hosted platforms, and web-based container solutions.

V4.0 New Requirements

11.3.1.2.a Examine scan tool configurations to verify that authenticated scanning is used for internal scans, with sufficient privileges, for those systems that accept credentials for scanning.

11.3.1.2.b Examine scan report results and interview personnel to verify that authenticated scans are performed.

11.3.1.2.c If accounts used for authenticated scanning can be used for interactive login, examine the accounts and interview personnel to verify the accounts are managed following all elements specified in Requirement 8.2.2.

11.3.1.2.d Examine documentation to verify that systems that are unable to accept credentials for authenticated scanning are defined.

8.2.2 Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary, on an exception basis, and are managed as follows:

- Account use is prevented unless needed for an exceptional circumstance.
- Use is limited to the time needed for the exceptional circumstance.
- Business justification for use is documented.
- Use is explicitly approved by management.
- Individual user identity is confirmed before access to an account is granted.
- Every action taken is attributable to an individual user.

The changes to Requirement 11.3.1.2 in the PCI V4.0 standard are a best practice until the requirements become mandatory after March 31, 2025. When the future dated requirements become mandatory, authenticated scanning must be performed from that point on.

Example: If your organization started its assessment in June of 2025, you would be required to provide quarterly internal authenticated vulnerability scans between April 1, 2025, and the due date of your report. The vulnerability scans before March 31, 2025, can be unauthenticated.

Timeline at a Glance

Here is a summary of the important implementation timeline dates for PCI V4.0:

- PCI V4.0 was released on March 31, 2022.
- Transition period is from March 31, 2022, through March 31, 2024. The transition period is the period where an organization's Cardholder Data Environment (CDE) can be assessed using PCI DSS v3.2.1 or V4.0.
- PCI v3.2.1 retires on March 31, 2024. After this date, V4.0 is mandatory.
- Future dated new requirements are mandatory after March 31, 2025.

BDO USA Can Help

As a Qualified Security Assessor Company (QSAC), BDO USA has experienced QSAs who can assist your organization in understanding and transitioning to the new PCI V4.0 standards.

HAVE QUESTIONS OR WANT TO LEARN MORE? CONTACT US!

GREG SCHU
Cybersecurity, Compliance, and Assessments Services Principal
gschu@bdo.com

BRIAN HILL
Cybersecurity, Compliance, and Assessments Services Managing Director
bhill@bdo.com

FRED BRANTNER
Cybersecurity, Compliance, and Assessments Services Director
fbrantner@bdo.com

JAMES ROMAN
Cybersecurity, Compliance, and Assessments Services Senior Manager
james.roman@bdo.com