QualysGuard® PCI Compliance Changes Frequently Asked Questions

August 5, 2010

Contents

PCI ASV Requirements

Why is Qualys changing QualysGuard PCI Compliance?

The PCI Security Standards Council (PCI SSC) released new Approved Scanning Vendor (ASV) requirements on March 16, 2010; these changes are detailed here. These new requirements contain significant changes to the existing Payment Card Industry Data Security Standard (PCI DSS) 11.2 External Scanning process that must be implemented by all ASVs by September 2010. Qualys is an ASV and will be updating QualysGuard PCI to support these new requirements.

Where can I obtain a copy of the ASV requirements?

The complete ASV 1.2 specification can be found here:
https://www.pcisecuritystandards.org/security_standards/docs/asv_validation_requirements.doc

The PCI SSC provides all documentation here:
https://www.pcisecuritystandards.org/security_standards/pci_dss_supporting_docs.shtml

Scanning Process

What changes will occur in the scanning process?

The actual scanning process will be unaffected by the changes in the specification. Certain workflows in the PCI Compliance application will change to assist customers in identifying IPs that are in-scope for PCI assessment.

What extra information do I need to provide?

In order to ensure accurate scanning, QualysGuard PCI Compliance scoping wizards will allow customers to submit URLs for in-scope payment processing applications and to provide details on load balancer configuration.

Reporting

How has scoring changed?

The specification requires that all vulnerabilities use CVSS v2 Base Scores to assign a severity of *High*, *Medium*, or *Low* to all vulnerabilities. The table below shows the methodology for determining the severity, although some vulnerabilities use specialized scoring; Denial-of-Service vulnerabilities, for example, do not cause a failure.

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.

How are CVSS v2 Base Scores determined?

Qualys uses NIST NVD-provided CVSS v2 Base Scores for most PCI-relevant vulnerabilities. Some vulnerabilities do not have NIST NVD CVSS v2 Base Scores provided; for these Qualys uses the CVSS v2 Base Score Formula as documented here: http://www.first.org/cvss/cvss-guide.html#i3.2.

How will the PASS/FAIL status of vulnerabilities be affected?

The PASS/FAIL status of most vulnerabilities will not change. The specification mandates that some vulnerabilities be considered automatic failures, such as the presence of either Internet-accessible database servers or obsolete/unsupported operating systems such as Windows XP SP2. Additionally, certain vulnerabilities that did not have CVSS v2 scores assigned from NIST NVD and were scored using the Qualys severity will now be scored using Qualys-calculated CVSS v2 scores. Please see Appendix A below.

How does the requirement to document potential vulnerabilities affect me?

QualysGuard PCI customers will see no changes as a result of this requirement. QualysGuard PCI will continue to accurately detect both Confirmed and Potential vulnerabilities and provide all the required information to investigate and remediate these issues.

What are the items listed in the Special Notes section?

Special Notes are to be used to disclose the presence of certain software that may pose a risk to the scan customer's environment due to insecure implementation rather than an exploitable vulnerability. Items that must be documented in the Special Notes section include cases where the customer cannot certify the configuration synchronization of systems behind load balancers and when Internet-accessible Point-of-Sale software is detected.

Are items in Special Notes considered non-compliant?

No. Special Notes items must be documented but do not impact compliance results.

Why am I required to document changes in my IPs?

The specification requires that "ASVs must minimally perform the below actions to identify if any scoping discrepancies exist in the information provided by the customer." QualysGuard PCI will remember any previously-scanned IP addresses and provides a wizard that allows customers to document why any changes occurred (such as systems retired or removed from payment processing) in order to comply with this requirement.

What is an attestation?

The specification requires that both scan customers and ASVs are required to submit written statements (known as attestations) confirming that reports conform to PCI DSS requirements for scoping, false positive documentation, and scan completeness.

What must the customer attestation contain?

The customer attestation must state the following:

> *(Scan customer name) attests that: This scan includes all components which should be in scope for PCI DSS, any component considered out-of-scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions is accurate and complete. (Scan customer name) also acknowledges the following: 1) proper scoping of this external scan is my responsibility, and 2) this scan result only indicates*

whether or not my scanned systems are compliant with the external vulnerability scan requirement of the PCI DSS; this scan result does not represent (Scan customer name)'s my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

What must the ASV attestation contain?

The ASV attestation must state the following:

> *(ASV name) attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, and 3) active interference. This report and any exceptions were reviewed by (name).*

What are "False Positives"?

The scan customer may dispute the findings in the ASV scanning report including vulnerabilities that are incorrectly found (false positives), those that have a disputed Common Vulnerability Scoring System (CVSS) Base Score, and vulnerabilities for which a compensating control is in place. In the event of a dispute the customer must provide supporting evidence for the dispute, and the ASV must review the provided evidence for relevance and accuracy. If approved by the ASV, the vulnerabilities disputed will not be used in the determination of compliance.

Why do I have to resubmit False Positives?

The specification states:

> *[The ASV may] not carry dispute findings forward from one quarterly scan to the next by the ASV. Dispute evidence must be verified/resubmitted by scan customer and evaluated again by the ASV for each quarterly scan.*

QualysGuard PCI will store all submitted false positives; if the same issue is found in future scans (after one quarter) the customer will be able to view and resubmit the evidence.

Why can't I get my certified report immediately?

The specification requires that the ASV review and approve all customer scoping information, attestations, and false positive documentation; once this review is complete the ASV must provide their own attestation of the validity of the process and report. This review will be completed within the published SLA for the ASV, at which point the certified report will be available for download.

QualysGuard Enterprise/Express/Consultant

Can I still use QualysGuard Enterprise PCI to perform my scanning?

Yes. QualysGuard Enterprise users may continue to use the PCI Option Profile with external scanners in order to perform PCI scans.

Why do I have to use QualysGuard PCI Compliance to generate a certified report?

The specification includes a number of changes to the workflow for PCI report generation, including the requirement for attestations and quarterly review of false positive documentation. The QualysGuard PCI application is customized to address these workflows. QualysGuard Enterprise users for PCI will have integrated access to QualysGuard PCI to perform these new workflow activities so that a certified report can be generated.

What do I need to do to use QualysGuard PCI from my QualysGuard Enterprise account?

QualysGuard Enterprise users will be required to perform an initial association of their subscription with QualysGuard PCI accounts; these accounts may be provisioned though the QualysGuard Enterprise interface. Once the initial association is created, QualysGuard Enterprise users will have integrated capabilities to move PCI scan results into the QualysGuard PCI workflow and generate certified reports.

Appendix A – QIDs with Revised Scores

The list below represents all QIDs that have newly calculated CVSS v2 scores of 4.0 or higher and will cause an IP to be marked as FAIL.

QID	Title
86658	Account Brute Force Possible Through IIS localstart.asp Authentication Interface
86657	Account Brute Force Possible Through IIS Printers Directory Authentication Interface
10444	Allaire JRun JSP Source Disclosure Vulnerability
10852	Allaire Macromedia ColdFusion Debug Mode Information Disclosure Vulnerability
12373	Apache Axis2 “xsd” Parameter Directory Traversal Vulnerability
11075	Apache mod_perl Apache::Status Page Accessible Vulnerability
86629	Apache mod_perl Module File Descriptor Leakage Vulnerability
12376	ASP.NET DEBUG Method Enabled Security Issue
86729	AutoComplete Attribute Not Disabled for Password in Form Based Authentication
86472	BEA WebLogic Hostname/NetBIOS Name Remote Information Disclosure Vulnerability
38510	CA Agent Discloses Exact Operating System Version
38211	Cisco CallManager tftp Accessible Vulnerability
43160	Cisco Global Site Selector Appliances DNS Vulnerability
43168	Cisco IOS Software Internet Key Exchange Resource Exhaustion Vulnerability
43159	Cisco IOS Software Mobile IP and Mobile IPv6 Vulnerabilities
43156	Cisco IOS Software Multiple Features Crafted TCP Sequence Vulnerability
43155	Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability
43180	Cisco IOS Software Multiprotocol Label Switching Packet Vulnerability
43175	Cisco IOS Software NAT Skinny Call Control Protocol Vulnerability
43166	Cisco IOS Software Network Time Protocol Packet Vulnerability (cisco-sa-20090923-ntp)
43154	Cisco IOS Software WebVPN and SSLVPN Vulnerabilities (cisco-sa-20090325-webvpn)
43165	Cisco IOS Software Zone-Based Policy Firewall Vulnerability (cisco-sa-20090923-ios-fw)
12311	CUPS Kerberos Cross-Site Scripting Vulnerability
38274	CVS PServer CVSROOT Obtained Through Bruteforcing
86717	CVS/Entries Accessible to Unauthenticated Remote Users
15035	DNS Server Allows Remote Clients to Snoop the DNS Cache
11033	Ecometry SGDynamo Absolute Path Disclosure Vulnerability
12087	Expose_php Set to On in php.ini
86645	FrontPage Extensions Configuration Information Obtained
45002	Global User List
19002	Guessed Oracle Database Name
11	Hidden RPC Services
86881	HP System Management Homepage "RedirectUrl" Parameter URI Redirection Vulnerability
86742	IBM WebSphere Application Server Multiple Remote Vulnerabilities
10927	IIS Sample Application Web Root Absolute Path Disclosure
10176	iisadmin Directory Present Vulnerability
38262	Internal/Private DNS Server's DNS Hierarchy Traced
86475	iPlanet Web Server Information Disclosure Vulnerability

QID	Title
86198	Jakarta Tomcat 3.2.1 Error Message Information Disclosure Vulnerability
82059	Kernel Memory Disclosure in ICMP Port Unreachable Packet Vulnerability
74245	MDaemon Mailing List Subscription Directory Traversal Vulnerability
12034	Microsoft ASP.NET Custom Errors Found Turned Off
12011	Microsoft ASP.NET Exception Stack Trace Remotely Accessible
12073	Microsoft ASP.NET Malformed Cookie Information Disclosure
10847	Microsoft ASP.NET Path Disclosure Vulnerability
12012	Microsoft ASP.NET Web Services Application Trace Remotely Accessible
90527	Microsoft Server Message Block Remote Code Execution Vulnerability (MS09-050)
10485	Microsoft Site Server 3.0 Weak LDAP_Anonymous Password Generation Vulnerability
50078	Microsoft SMTP Fails To Understand Pipelined Commands in DATA
66036	mountd RPC Daemon Discloses Exported Directories Accessed by Remote Hosts
12114	MRTG Traffic Load Monitor Present
19551	MySQL "UNINSTALL PLUGIN" Security Bypass Vulnerability
19560	MySQL Multiple Vulnerabilities
38284	Netscape/OpenSSL Cipher Forcing Bug
38293	NTP Information Disclosure Vulnerability
86711	NULL Byte Poison Information Disclosure Vulnerability
19017	Oracle Listener Discloses Absolute Path and Environment Variables
12365	PHP “ext/phar/stream.c” and “ext/phar/dirstream.c” Multiple Format String Vulnerabilities
12384	PHP “strrchr()” Function Information Disclosure Vulnerability
12357	PHP HTTP Chunked Encoding Processing Signedness - Zero Day
12318	PHP Versions Prior to 5.2.12 Multiple Vulnerabilities
11252	PHP-Banner Exchange Path Disclosure Vulnerability
11253	PHP-Nuke Private Messages Module Path Disclosure Vulnerability
11325	pMachine Remote Path Disclosure Vulnerability
1112	Potential Litmus Backdoor Detected
10199	Potential Misuse of Squid cachemgr.cgi
10178	printenv Script
117865	RealNetworks Helix Server Multiple Remote Code Execution Vulnerabilities
15020	Reverse DNS Name Resolution Discloses Private Network Addresses
27317	Serv-U FTP Server Multiple Vulnerabilities
38435	SIP Users Information Disclosure
38171	SSL Certificate - Server Public Key Too Small
78028	Sun Process List (ps -ef)
10214	Suspicious Script file.pl
74045	Valid Logins Guessed with SMTP EXPN Command
74046	Valid Logins/Aliases Guessed with SMTP VRFY Command
86445	Web Directories Listable Vulnerability
86400	Web Server Reveals Absolute Path
86763	Web Server Uses Plain Text Basic Authentication
86241	WebDAV HTTP Method “PROPFIND” Enabled
27029	Windows Configuration Files Present on Anonymous FTP Server Vulnerability

QID	Title
27020	Word Documents Present on Anonymous FTP Server Vulnerability
12307	WordPress #wp-config.php# Backup Is Readable
12309	WordPress META-Generator Header Indicates Vulnerable Version
12310	WordPress README.html Indicates Vulnerable Version
12308	WordPress RSS META-Generator Header Indicates Vulnerable Version
12306	WordPress wp-config.php~ Backup Is Readable
11311	Wordtrans PhpInfo Information Disclosure
66013	ypbind RPC Daemon Present Vulnerability