Qualys. PCI

Powered by Qualys.

Payment Card Industry (PCI) Technical Report

02/06/2026

ASV Scan Report Attestation of Scan Compliance

A.1 Scan Customer Information				A.2 Approved Scanning Vendor Information			
Company:	BCH Digital			Company:	Qualys		
Contact Name:	Chris Johnson	Job Title:	Technical Manager	Contact Name:	Qualys PCI Support	Job Title:	Qualys PCI Support
Telephone:	01614704535	Email:	asv+bchdigital@uk.clara.net	Telephone:	+1(866)801-6161	Email:	support@qualys.com
Business Address:	Suite 3a, 127 Portland Street			Business Address:	919 E Hillsdale Blvd, 4th Floor		
City:	Manchester	State/Province:	None	City:	Foster City	State/Province:	California
ZIP/postal code:	M1 2HY	Country:	United Kingdom	ZIP/postal code:	94404	Country:	United States of America
URL:				URL:	http://www.qualys.com/		

A.3 Scan Status			
Date scan completed	02/06/2026	Scan expiration date (90 days from date scan completed)	05/07/2026
Compliance Status	PASS	Scan report type	Full scan
Number of unique in-scope components scanned			1
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

A.4 Scan Customer Attestation

BCH Digital attests on 02/06/2026 at 15:44:33 GMT that this scan (either by itself or combined with multiple, partial, or failed scans/rescans, as indicated in the above Section A.3, "Scan Status") 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 - including compensating controls if applicable - is accurate and complete.
BCH Digital also acknowledges 1) accurate and complete 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 PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

A.5 ASV Attestation

This scan and report was prepared and conducted by Qualys under certificate number 3728-01-20, according to internal processes that meet PCI DSS requirement 11.3.2 and the ASV Program Guide.
Qualys 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, 3) compensating controls (if applicable), and 4) active scan interference. This report and any exceptions were reviewed by Qualys PCI Support

ASV Scan Report Summary

Part 1. Scan Information

Scan Customer Company:	BCH Digital	ASV Company:	Qualys
Date scan was completed:	02/06/2026	Scan expiration date:	05/07/2026

Part 2. Component Compliance Summary

18.169.252.70, ec2-18-169-252-70.eu-west-2.compute.amazonaws.com	PASS

Part 2. Component Compliance Summary - (Hosts Not Current)

Part 3a. Vulnerabilities Noted for each Component

Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
-	-	-	-	-	-

Part 3b. Special Notes to Scan Customer by Component

Component	Special Note to Scan Customer	Item Noted	Per section 7.2 of the ASV Program Guide, scan customer's description of action taken and declaration that software is either needed for business and implemented securely, or removed
-	-	-	-

Part 3c. Special Notes Full Text

Note

-

Part 4a. Scope Submitted by Scan Customer for Discovery

IP Addresses/ranges/subnets, domains, URLs, etc.

3.8.57.112, 3.11.168.144, 13.42.75.60, 13.43.3.252, 18.132.240.137, 18.134.203.3, 18.135.203.175, 18.169.252.70, 35.176.49.71, 35.179.235.122, 51.24.57.65

Part 4b. Scan Customer Designated "In-Scope" Components (Scanned)

IP Addresses/ranges/subnets, domains, URLs, etc.

18.169.252.70, ec2-18-169-252-70.eu-west-2.compute.amazonaws.com

Part 4c. Scan Customer Designated "Out-of-Scope" Components (Not Scanned)

IP Addresses/ranges/subnets, domains, URLs, etc.

IP Addresses/Ranges : - (not active) Scan customer attests that this IP address is not issued/assigned to any physical or virtual host. ASV confirmed it is nonresponsive.

Report Summary	
Company:	BCH Digital
Hosts in Account:	11 IP
Hosts Active:	1
Hosts Scanned:	11
Scan Date:	02/06/2026 at 09:03:13 GMT
Report Date:	02/06/2026 at 15:44:37 GMT
Report Title:	ASV BCH Digital Attested pass report February 2026
Template Title:	Payment Card Industry (PCI) Technical Report

Summary of Vulnerabilities

Vulnerabilities Total	8	Average Security Risk	0.0

by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	0	0	0	0
2	0	0	0	0
1	0	0	8	8
Total	0	0	8	8

by PCI Severity			
PCI Severity	Confirmed	Potential	Total
High	0	0	0
Medium	0	0	0
Low	0	0	0
Total	0	0	0

Vulnerabilities by PCI Severity

Potential Vulnerabilities by PCI Severity

Vulnerabilities by Severity

Potential Vulnerabilities by Severity

There is no data available

Detailed Results

18.169.252.70 (ec2-18-169-252-70.eu-west-2.compute.amazonaws.com,-)

Vulnerabilities Total	8	Security Risk	0.0

Information Gathered (8)

ICMP Replies Received

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 82040
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/16/2003

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.

We have sent the following types of packets to trigger the host to send us ICMP replies:

Echo Request (to trigger Echo Reply)
Timestamp Request (to trigger Timestamp Reply)
Address Mask Request (to trigger Address Mask Reply)
UDP Packet (to trigger Port Unreachable Reply)
IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)

Listed in the "Result" section are the ICMP replies that we have received.

RESULT:

ICMP Reply Type	Triggered By	Additional Information
Echo (type=0 code=0)	Echo Request	Echo Reply

DNS Host Name

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 6
Category: Information gathering

CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 01/04/2018

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

RESULT:

IP address	Host name
18.169.252.70	ec2-18-169-252-70.eu-west-2.compute.amazonaws.com

Traceroute

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 45006
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 05/09/2003

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

RESULT:

Hops	IP	Round Trip Time	Probe	Port
1	140.91.222.78	0.40ms	ICMP	
2	72.21.221.57	1.09ms	ICMP	
3	*.*.*.*	0.00ms	Other	80
4	*.*.*.*	0.00ms	Other	80
5	*.*.*.*	0.00ms	Other	80
6	*.*.*.*	0.00ms	Other	80
7	*.*.*.*	0.00ms	Other	80
8	18.169.252.70	8.15ms	ICMP	

Target Network Information

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 45004
Category: Information gathering
CVE ID: -
Vendor Reference: -

Bugtraq ID: -
Last Update: 08/15/2013

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

RESULT:

The network handle is: NET-18-168-0-0-1
Network description:
Amazon Data Services UK AMAZON-LHR

Internet Service Provider

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 45005
Category: Information gathering
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 09/27/2013

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

RESULT:

The ISP network handle is: NET-140-91-0-0-2
ISP Network description:
Oracle Public Cloud OC-195

Host Names Found

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	08/27/2020

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

RESULT:

Host Name	Source
ec2-18-169-252-70.eu-west-2.compute.amazonaws.com	FQDN

Host Scan Time - Scanner

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	09/15/2022

THREAT:
The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

RESULT:

Scan duration: 2509 seconds

Start time: Fri, Feb 06 2026, 09:06:09 GMT

End time: Fri, Feb 06 2026, 09:47:58 GMT

Firewall Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	04/22/2019

THREAT:
A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

RESULT:

Some of the ports filtered by the firewall are: 20, 21, 22, 23, 25, 53, 80, 111, 135, 443.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-112,114-381,383-1559,1561-1705,1707-1721,1723-1999,2001-2033,2035,2037-2100,
2102-2146,2148-2512,2514-2701,2703-3388,3390-5491,5493-5504,5506-5549,
5551-5559,5561-5569,5571-5579,5581-5630,5632-6013,6015-6128,6130-7006,
7008-7009,7011-9098,9100-9989,9991-10109,10111-42423,42425-65535

Appendices

Hosts Scanned

18.169.252.70

Hosts Not Alive

3.8.57.112,3.11.168.144,13.42.75.60,13.43.3.252,18.132.240.137,18.134.203.3,18.135.203.175,35.176.49.71,35.179.235.122,51.24.57.65

Option Profile

Scan

Scanned TCP Ports:	Full
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	Off
Load Balancer Detection:	Off
Password Brute Forcing:	Standard
Vulnerability Detection:	Complete
Windows Authentication:	Disabled
SSH Authentication:	Disabled
Oracle Authentication:	Disabled
SNMP Authentication:	Disabled
Perform 3-way Handshake:	Off

Advanced

Hosts Discovery:	TCP Standard Scan, UDP Standard Scan, ICMP On
Ignore RST packets:	Off
Ignore firewall-generated SYN-ACK packets:	Off
Do not send ACK or SYN-ACK packets during host discovery:	Off

Report Legend

Payment Card Industry (PCI) Status

The Detailed Results section of the report shows all detected vulnerabilities and potential vulnerabilities sorted by host. The vulnerabilities and potential vulnerabilities marked PCI FAILED caused the host to receive the PCI compliance status FAILED. All vulnerabilities and potential vulnerabilities marked PCI FAILED must be remediated to pass the PCI compliance requirements. Vulnerabilities not marked as PCI FAILED display vulnerabilities that the PCI Compliance service found on the hosts when scanned. Although these vulnerabilities are not in scope for PCI, we do recommend that you remediate the vulnerabilities in severity order.

A PCI compliance status of PASSED for a single host/IP indicates that no vulnerabilities or potential vulnerabilities, as defined by the PCI DSS compliance standards set by the PCI Council, were detected on the host. An overall PCI compliance status of PASSED indicates that all hosts in the report passed the PCI compliance standards.

A PCI compliance status of FAILED for a single host/IP indicates that at least one vulnerability or potential vulnerability, as defined by the PCI DSS compliance standards set by the PCI Council, was detected on the host. An overall PCI compliance status of FAILED indicates that at least one host in the report failed to meet the PCI compliance standards.

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Severity	Level	Description
LOW	Low	A vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
MED	Medium	A vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
HIGH	High	A vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.

3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Severity	Level	Description
LOW	Low	A potential vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
MED	Medium	A potential vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
HIGH	High	A potential vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.