

Attestation of Scan Compliance

A.1 Scan Custome	er Information			A.2 Approved Sca	nning Vendor Inform	nation	
Company:	RCHILLI INC			Company:	Trustwave Holdings,	Inc.	
Contact Name:	Vinay Johar	Job Title:		Contact Name:	Trustwave Support	Job Title:	
Telephone:	408.201.9444	E-mail: vinay@	rchilli.com	Telephone:	1-800-363-1621	E-mail:	support@trustwave.com
Business Address:	2603 Camino Ramon Ste 2	72		Business Address:	70 West Madison St., Ste 1050		
City:	San Ramon	State/Province:	California	City:	Chicago	State/Province:	IL
ZIP/Postal Code:	94583	Country:	US	ZIP/Postal Code:	60602	Country:	US
Website / URL:				Website / URL:	www.trustwave.com		
A.3 Scan Status							
Date scan completed:	2020-05-18	Scan expiration da completed):	te (90 days from date scan	2020-08-18			
Compliance status:	Pass	Scan report type:	Full Scan				
Number of unique in-sc	ope components scanned	:	2				
Number of identified fa	iling vulnerabilities:		0				
	found by ASV but not sca ed they were out of scope:		0				
A.4 Scan Custome	er Attestation			A.5 ASV Attestation	on		

RCHILLI INC attests on 2020-05-18 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. RCHILLI INC 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.

Signature	Printed Name
Title	Date

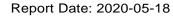
This scan and report was prepared and conducted by Trustwave under certificate number 3702-01-14 (2019), 3702-01-13 (2018), 3702-01-12 (2017), 3702-01-11 (2016), 3702-01-10 (2015), 3702-01-09 (2014), 3702-01-08 (2013), 3702-01-07 (2012), 3702-01-06 (2011), 3702-01-05 (2010), according to internal processes that meet PCI DSS Requirement 11.2.2 and the ASV Program Guide.

Trustwave 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 the Trustwave Quality Assurance Process.



Vulnerability Scan Report: Table of Contents

Attes	tation of Scan Compliance	1
ASV S	can Report Summary	4
	Part 1. Scan Information	4
	Part 2. Component Compliance Summary	4
	Part 3a. Vulnerabilities Noted for Each Component	4
	Part 3b. Special Notes by Component	4
	Part 3c. Special Notes - Full Text	5
	Part 4a. Scope Submitted by Scan Customer for Discovery	5
	Part 4b. Scan Customer Designated "In-Scope" Components (Scanned)	5
	Part 4c. Scan Customer Designated "Out-of-Scope" Components (Not Scanned)	5
ASV S	can Report Vulnerability Details	7
	Part 1. Scan Information	7
	Part 2. Vulnerability Details	7
	34.107.233.166	7





Attestation of Scan Compliance



ASV Scan Report Summary

Part 1. Scan Information

Scan Customer Company	RCHILLI INC	ASV Company	Trustwave Holdings, Inc.
Date Scan Completed	2020-05-18	Scan Expiration Date	2020-08-16

Part 2. Component Compliance Summary

Component (IP Address, domain, etc):

34.107.233.166

rest.rchilli.com

Pass

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)
34.107.233.166	Enumerated Hostnames	Info	0.00	Pass	
34.107.233.166	Enumerated SSL/TLS Cipher Suites	Info	0.00	Pass	
34.107.233.166	Potential HTTP Caching Server	Info	0.00	Pass	
34.107.233.166	SSL-TLS Certificate Information	Info	0.00	Pass	Note to scan customer: This vulnerability is not recognized in the National Vulnerability Database.
34.107.233.166	TLSv1.2 Supported	Info	0.00	Pass	
34.107.233.166	Wildcard SSL Certificate Detected	Info	0.00	Pass	
	34.107.233.166 34.107.233.166 34.107.233.166 34.107.233.166	34.107.233.166 Enumerated Hostnames 34.107.233.166 Enumerated SSL/TLS Cipher Suites 34.107.233.166 Potential HTTP Caching Server 34.107.233.166 SSL-TLS Certificate Information 34.107.233.166 TLSv1.2 Supported 34.107.233.166 Wildcard SSL Certificate	34.107.233.166 Enumerated Hostnames Info 34.107.233.166 Enumerated SSL/TLS Cipher Suites 34.107.233.166 Potential HTTP Caching Server Info 34.107.233.166 SSL-TLS Certificate Information Info 34.107.233.166 TLSv1.2 Supported Info 34.107.233.166 Wildcard SSL Certificate Info	Component Level Score 34.107.233.166 Enumerated Hostnames Info 0.00 34.107.233.166 Enumerated SSL/TLS Cipher Suites Info 0.00 34.107.233.166 Potential HTTP Caching Server Info 0.00 34.107.233.166 SSL-TLS Certificate Information Info 0.00 34.107.233.166 TLSv1.2 Supported Info 0.00 34.107.233.166 Wildcard SSL Certificate Info 0.00	Component Level Score Status 34.107.233.166 Enumerated Hostnames Info 0.00 Pass 34.107.233.166 Enumerated SSL/TLS Cipher Suites Info 0.00 Pass 34.107.233.166 Potential HTTP Caching Server Info 0.00 Pass 34.107.233.166 SSL-TLS Certificate Information Info 0.00 Pass 34.107.233.166 TLSv1.2 Supported Info 0.00 Pass 34.107.233.166 Wildcard SSL Certificate Info 0.00 Pass

Consolidated Solution/Correction Plan for the above Component:



ASV Scan Report Summary

Part 3b. Special Notes by Component

Component

Special Note

Item Noted

Scan customer's description of action taken and declaration that software is either implemented securely or removed

No Special Notes

Part 3c. Special Notes - Full Text

Note

Customer Note

Customer has not validated that all servers behind load balancers are identical and synchronized.

Part 4a. Scope Submitted by Scan Customer for Discovery

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

Domain: rest.rchilli.com

IP Address: 34.107.233.166

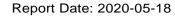
Part 4b. Scan Customer Designated "In-Scope" Components (Scanned)

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

34.107.233.166 / 166.233.107.34.bc.googleusercontent.com (34.107.233.166)

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

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





ASV Scan Report Summary

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

Copyright © 2020 Trustwave Holdings, Inc., All rights reserved.



ASV Scan Report Vulnerability Details

Part 1. Scan Information

Scan Customer Company	RCHILLI INC	ASV Company	Trustwave Holdings, Inc.
Date Scan Completed	2020-05-18	Scan Expiration Date	2020-08-16

Part 2. Vulnerability Details

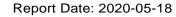
The following issues were identified during this scan. Please review all items and address all that items that affect compliance or the security of your system.

In the tables below you can find the following information about each TrustKeeper finding.

- CVE Number The Common Vulnerabilities and Exposure number(s) for the detected vulnerability an industry standard for cataloging vulnerabilities. A comprehensive list of CVEs can be found at nvd.nist.gov or cve.mitre.org.
- · Vulnerability This describes the name of the finding, which usually includes the name of the application or operating system that is vulnerable.
- CVSS Score The Common Vulnerability Scoring System is an open framework for communicating the characteristics and impacts of IT vulnerabilities. Further
 information can be found at www.first.org/cvss or nvd.nist.gov/cvss.cfm.
- · Severity This identifies the risk of the vulnerability. It is closely associated with the CVSS score.
- Compliance Status Findings that are PCI compliance violations are indicated with a Fail status. In order to pass a vulnerability scan, these findings must be addressed.
 Most findings with a CVSS score of 4 or more, or a Severity of Medium or higher, will have a Fail status. Some exceptions exist, such as DoS vulnerabilities, which are not included in PCI compliance.
- Details TrustKeeper provides the port on which the vulnerability is detected, details about the vulnerability, links to available patches and other specific guidance on actions you can take to address each vulnerability.

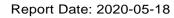
For more information on how to read this section and the scoring methodology used, please refer to the appendix.

34.107.2	34.107.233.166							
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details		
1		Potential HTTP Caching Server	0.00	Info	Pass	Port: tcp/80 The scanner has determined that an HTTP caching server lies between		



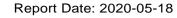


34.107.2	34.107.233.166							
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details		
						the remote HTTP server and the scanner. This is done via the detection of the 'Via' and 'X-Cache' HTTP headers.		
						CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http		
						Evidence: Via Header: 1.1 google		
						Remediation: Nothing needs to be done. This is for informational purposes only.		
2		Wildcard SSL Certificate Detected	0.00	Info	Pass	Port: tcp/443 An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service. CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http Evidence: Subject: /CN=*.rchilli.com Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=RapidSSL RSA CA 2018 Certificate Chain Depth: 0		
						Wildcard Subject Name: *.rchilli.com Remediation: Review your certificate configurations to assure that wildcard certificates are suitable for your application.		



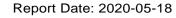


34.107.2	233.166					
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
3		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	Port: tcp/443 The finding reports the SSL cipher suites for each SSL/TLS service version provided by the remote service. This finding does not represent a vulnerability, but is only meant to provide visibility into the behavior and configuration of the remote SSL/TLS service. The information provided as part of this finding includes the SSL version (ex: TLSv1) as well as the name of the cipher suite (ex: RC4-SHA). A cipher suite is a set of cryptographic algorithms that provide authentication, encryption, and message authentication code (MAC) as part of an SSL/TLS negotiation and through the lifetime of the SSL session. It is typical that an SSL service would support multiple cipher suites. A cipher suite can be supported by across multiple SSL/TLS versions, so you should be of no concern to see the same cipher name reported for multiple CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http Reference: http://www.openssl.org/docs/apps/ciphers.html Evidence: Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA





34.107.2	233.166					
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: No remediation is necessary.
4		SSL-TLS Certificate Information	0.00	Info	Pass	Port: tcp/443 Information extracted from a certificate discovered on a TLS or SSL wrapped service. CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http Evidence: Verified: true Today: 2020-05-18 07:14:18 -0500 Start date: 2019-01-15 00:00:00 UTC End date: 2021-02-06 12:00:00 UTC Expired: false Fingerprint: DD:4C:E2:7F:16:8F:7C:D7:51:B8:AD:F8:E0:91:D1:F4 Subject: /CN=*.rchilli.com Common name: *.rchilli.com Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=RapidSSL RSA CA 2018 Signature Algorithm: sha256WithRSAEncryption Version: 2
5		TLSv1.2 Supported	0.00	Info	Pass	Port: tcp/443 This service supports the use of the TLSv1.2 protocol.





34.107.	34.107.233.166								
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details			
						CVSSv2: AV:N/AC:H/Au:M/C:N/I:N/A:N Service: http Evidence: Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA			
6		Potential HTTP Caching Server	0.00	Info	Pass	Port: tcp/443 The scanner has determined that an HTTP caching server lies between the remote HTTP server and the scanner. This is done via the detection of the 'Via' and 'X-Cache' HTTP headers. CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http Evidence: Via Header: 1.1 google Remediation: Nothing needs to be done. This is for informational purposes only.			
7		Enumerated Hostnames	0.00	Info	Pass	This list contains all hostnames discovered during the scan that are believed to belong to this host. CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Evidence:			



34.107.233.166								
# CVE Number Vulnerability CVSS Score Severity Compliance Status Details								
Hostname: ro DNS Remediatio No action is r								