

Attestation of Scan Compliance

A.1 Scan Customer Information

Company: CanadaHelps CanaDon
Contact Name: Mike Stairs **Job Title:**
Telephone: 416 628 6948 x2394 **E-mail:** mikes@canadahelps.org
Business Address: 355 Adelaide Street West Ground Floor
City: Toronto **State/Province:** Ontario
ZIP/Postal Code: M5V1S2 **Country:** CA
Website / URL:

A.2 Approved Scanning Vendor Information

Company: Trustwave Holdings, Inc.
Contact Name: Trustwave Support **Job Title:**
Telephone: 1-800-363-1621 **E-mail:** support@trustwave.com
Business Address: 70 West Madison St., Ste 1050
City: Chicago **State/Province:** IL
ZIP/Postal Code: 60602 **Country:** US
Website / URL: www.trustwave.com

A.3 Scan Status

Date scan completed:	2019-03-28	Scan expiration date (90 days from date scan completed):	2019-06-28
Compliance status:	Pass	Scan report type:	Full Scan
Number of unique in-scope components scanned:	2		
Number of identified failing vulnerabilities:	0		
Number of components found by ASV but not scanned because scan customer confirmed they were out of scope:	0		

A.4 Scan Customer Attestation

CanadaHelps CanaDon attests on 2019-02-21 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. CanadaHelps CanaDon 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

Title

Printed Name

Date

A.5 ASV Attestation

This scan and report was prepared and conducted by Trustwave under certificate number 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

Attestation of Scan Compliance	1
ASV Scan 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	5
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)	6
Part 4c. Scan Customer Designated "Out-of-Scope" Components (Not Scanned)	6
ASV Scan Report Vulnerability Details	7
Part 1. Scan Information	7
Part 2. Vulnerability Details	7
52.233.56.161 (token.canadahelps.org)	7
172.86.186.99 (www.canadahelps.org)	11

Attestation of Scan Compliance

ASV Scan Report Summary

Part 1. Scan Information

Scan Customer Company	CanadaHelps CanaDon	ASV Company	Trustwave Holdings, Inc.
Date Scan Completed	2019-03-28	Scan Expiration Date	2019-06-26

Part 2. Component Compliance Summary

Component (IP Address, domain, etc):	52.233.56.161 - token.canadahelps.org (token.canadahelps.org)	Pass
Component (IP Address, domain, etc):	172.86.186.99 - www.canadahelps.org (www.canadahelps.org)	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)
1	52.233.56.161 (token.canadahelps.org)	Enumerated Applications	Info	0.00	Pass	Note to scan customer: This vulnerability is not recognized in the National Vulnerability Database.
2	52.233.56.161 (token.canadahelps.org)	Enumerated Hostnames	Info	0.00	Pass	
3	52.233.56.161 (token.canadahelps.org)	Enumerated SSL/TLS Cipher Suites	Info	0.00	Pass	
4	52.233.56.161 (token.canadahelps.org)	SSL Perfect Forward Secrecy Supported	Info	0.00	Pass	
5	52.233.56.161 (token.canadahelps.org)	SSL-TLS Certificate Information	Info	0.00	Pass	Note to scan customer: This vulnerability is not recognized in the National Vulnerability Database.

ASV Scan Report Summary

#	Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls (Noted by the ASV for this vulnerability)
Consolidated Solution/Correction Plan for the above Component:						
6	172.86.186.99 (www.canadahelp.s.org)	Enumerated Applications	Info	0.00	Pass	Note to scan customer: This vulnerability is not recognized in the National Vulnerability Database.
Consolidated Solution/Correction Plan for the above Component:						

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

ASV Scan Report Summary

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

Domain: token.canadahelps.org

Domain: www.canadahelps.org

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

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

52.233.56.161 (token.canadahelps.org)

172.86.186.99 (www.canadahelps.org)

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

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

No Data

ASV Scan Report Vulnerability Details

Part 1. Scan Information

Scan Customer Company	CanadaHelps CanaDon	ASV Company	Trustwave Holdings, Inc.
Date Scan Completed	2019-03-28	Scan Expiration Date	2019-06-26

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.

52.233.56.161 (token.canadahelps.org)

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
1		SSL Perfect Forward Secrecy Supported	0.00	Info	Pass	Port: tcp/443 The server supports Ephemeral Diffie-Hellman ciphers for the SSL/TLS

ASV Scan Report Vulnerability Details

52.233.56.161 (token.canadahelps.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>key exchange phase. Using this algorithm enforces Forward Secrecy for secure communications with the server.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http Application: nginx:nginx</p> <p>Evidence: Cipher Suite: TLSv1_2 : DHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES128-GCM-SHA256</p> <p>Remediation: No remediation is necessary.</p>
2		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	<p>Port: tcp/443</p> <p>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).</p> <p>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</p>

ASV Scan Report Vulnerability Details

52.233.56.161 (token.canadahelps.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>versions, so you should be of no concern to see the same cipher name reported for multiple</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http Application: nginx:nginx</p> <p>Reference: http://www.openssl.org/docs/apps/ciphers.html</p> <p>Evidence: Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : AES128-GCM-SHA256</p> <p>Remediation: No remediation is necessary.</p>
3		SSL-TLS Certificate Information	0.00	Info	Pass	<p>Port: tcp/443</p> <p>Information extracted from a certificate discovered on a TLS or SSL wrapped service.</p>

ASV Scan Report Vulnerability Details

52.233.56.161 (token.canadahelps.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http Application: nginx:nginx Evidence: Verified: true Today: 2019-03-28 19:29:04 -0500 Start date: 2018-04-09 00:00:00 UTC End date: 2020-04-08 23:59:59 UTC Expired: false Fingerprint: 97:E1:D0:46:01:10:01:8C:6C:45:BC:92:5A:DF:8F:49 Subject: /OU=Domain Control Validated/OU=EssentialSSL/CN=token.canadahelps.org Common name: token.canadahelps.org Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO RSA Domain Validation Secure Server CA Signature Algorithm: sha256WithRSAEncryption Version: 2
4		Enumerated Applications	0.00	Info	Pass	Port: tcp/443 The following applications have been enumerated on this device. CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http Application: nginx:nginx Evidence:

ASV Scan Report Vulnerability Details

52.233.56.161 (token.canadahelps.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						CPE: nginx:nginx URI: / Version: 1.15.8 Remediation: No remediation is required.
5		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: Hostname: token.canadahelps.org, Source: SSL Certificate Subject Common Name Hostname: token.canadahelps.org, Source: SSL Certificate Subject subjectAltName DNS Hostname: www.token.canadahelps.org, Source: SSL Certificate Subject subjectAltName DNS Remediation: No action is required.

172.86.186.99 (www.canadahelps.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
1		Enumerated Applications	0.00	Info	Pass	Port: tcp/80

ASV Scan Report Vulnerability Details

172.86.186.99 (www.canadahelps.org)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						<p>The following applications have been enumerated on this device.</p> <p>CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N Service: http Application: nginx:nginx</p> <p>Evidence: CPE: nginx:nginx URI: / Version: 1.15.8</p> <p>Remediation: No remediation is required.</p>

ASV Feedback Form

This form is used to review ASVs and their work product, and is intended to be completed after a PCI Scanning Service by the ASV client. While the primary audience of this form are ASV scanning clients (merchants or service providers), there are several questions at the end, under "ASV Feedback Form for Payment Brands and Others," to be completed as needed by Payment Brand participants, banks, and other relevant parties. This form can be obtained directly from the ASV during the PCI Scanning Service, or can be found online in a usable format at <https://www.pcisecuritystandards.org>. Please send this completed form to PCI SSC at: asv@pcisecuritystandards.org.

ASV FEEDBACK FORM	
Client Name (merchant or service provider):	Approved Scanning Vendor Company (ASV):
Name	Name
Contact	Contact
Telephone	Telephone
E-Mail	E-Mail
Business location where assessment took place:	ASV employee who performed assessment:
Street	Name
City	Telephone
State/Zip	E-Mail
For each question, please indicate the response that best reflects your experience and provide comments.	
4 = Strongly Agree 3 = Agree 2 = Disagree 1 = Strongly Disagree	
1) During the initial engagement, did the ASV explain the objectives, timing, and review process, and address your questions and concerns?	
Response:	
Comments:	

2) Did the ASV employee(s) understand your business and technical environment, and the payment card industry?

Response:

Comments:

3) Did the ASV employee(s) have sufficient security and technical skills to effectively perform this PCI Scanning Service?

Response:

Comments:

4) Did the ASV sufficiently understand the PCI Data Security Standard and the PCI Security Scanning Procedures?

Response:

Comments:

5) Did the ASV effectively minimize interruptions to operations and schedules?

Response:

Comments:

6) Did the ASV provide an accurate estimate for time and resources needed?

Response:

Comments:

7) Did the ASV provide an accurate estimate for scan report delivery?

Response:

Comments:

8) Did the ASV attempt to market products or services for your company to attain PCI compliance?
Response:
Comments:
9) Did the ASV imply that use of a specific brand of commercial product or service was necessary to achieve compliance?
Response:
Comments:
10) In situations where remediation was required, did the ASV present product and/or solution options that were not exclusive to their own product set?
Response:
Comments:
11) Did the ASV use secure transmission to send any confidential reports or data?
Response:
Comments:
12) Did the ASV demonstrate courtesy, professionalism, and a constructive and positive approach?
Response:
Comments:
13) Was there sufficient opportunity for you to provide explanations and responses during the scans?
Response:
Comments:

14) During the review wrap-up, did the ASV clearly communicate findings and expected next steps?

Response:

Comments:

15) Did the ASV provide sufficient follow-up to address false positives until eventual scan compliance was achieved?

Response:

Comments:

Please provide any additional comments here about the ASV, your PCI Scanning Service, or the PCI documents.

ASV FEEDBACK FORM FOR PAYMENT BRANDS AND OTHERS**Name of ASV Client (merchant or service provider reviewed):****ASV Company Name:**

Payment Brand Reviewer:

ASV employee who performed assessment:

Name

Name

Telephone

Telephone

E-Mail

E-Mail

For each question, please indicate the response that best reflects your experience and provide comments.**4 = Strongly Agree 3 = Agree 2 = Disagree 1 = Strongly Disagree****1) Does the ASV clearly understand how to notify your payment brand about compliance and non-compliance issues, and the status of merchants and service providers?**

Response:

Comments:

2) Did you receive any complaints about ASV activities related to this scan?

Response:

Comments:

3) Did the ASV demonstrate sufficient understanding of the PCI Data Security Standard and the PCI Security Scanning Procedures?

Response:

Comments: