Trustwave®

Report Date: 2018-07-10

Attestation of Scan Compliance

A.1 Scan Customer Information

Company:	PEOPLEVINE		
Contact Name:	Jordan Gilman	**Job Title:**	
Telephone:	3125433399	**E-mail:**	jordan@peoplevine.com
Business Address:	222 Merchandise Mart Plaza Suite 1212 c/o 1871		
City:	CHICAGO	**State/Province:**	Illinois
ZIP/Postal Code:	60654	**Country:**	US
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:	2018-07-10	Scan expiration date (90 days from date scan completed):	2018-10-10
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 they were out of scope:	0

A.4 Scan Customer Attestation

PEOPLEVINE attests on 2018-07-10 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. PEOPLEVINE 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 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

Trustwave®

Report Date: 2018-07-10

ASV Scan Report Summary

Part 1. Scan Information

Scan Customer Company	PEOPLEVINE	ASV Company	Trustwave Holdings, Inc.
Date Scan Completed	2018-07-10	Scan Expiration Date	2018-10-08

Part 2. Component Compliance Summary

Component (IP Address, domain, etc):	168.62.224.239 - control.peoplevine.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)
1	168.62.224.239	Discovered HTTP Methods	Info	0.00	Pass	
2	168.62.224.239	Discovered Web Applications	Info	0.00	Pass	
3	168.62.224.239	Discovered Web Directories	Info	0.00	Pass	
4	168.62.224.239	Enumerated Applications	Info	0.00	Pass	**Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database.
5	168.62.224.239	Enumerated Hostnames	Info	0.00	Pass	
6	168.62.224.239	Enumerated SSL/TLS Cipher Suites	Info	0.00	Pass	
7	168.62.224.239	SSL-TLS Certificate Information	Info	0.00	Pass	**Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database.
8	168.62.224.239	URLScan Detected	Info	0.00	Pass	

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)
9	168.62.224.239	Wildcard SSL Certificate Detected	Info	0.00	Pass	

Consolidated Solution/Correction Plan for the above Component:

- Configure the HTTP service(s) running on this host to adhere to information security best practices.
- Restrict access to any files, applications, and/or network services for which there is no business requirement to be publicly accessible.

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
No Special Notes

Part 4a. Scope Submitted by Scan Customer for Discovery

IP Address/ranges/subnets, domains, URLs, etc.
Domain: control.peoplevine.com

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

ASV Scan Report Summary

IP Address/ranges/subnets, domains, URLs, etc.
168.62.224.239

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	PEOPLEVINE	ASV Company	Trustwave Holdings, Inc.
Date Scan Completed	2018-07-10	Scan Expiration Date	2018-10-08

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.

168.62.224.239						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
1		Enumerated Applications	0.00	Info	Pass	**Port:** tcp/80 The following applications have been enumerated on this device.

ASV Scan Report Vulnerability Details

168.62.224.239						
#	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:** microsoft:iis **Evidence:** CPE: microsoft:iis URI: / Version: 10.0 **Remediation:** No remediation is required.
2		Enumerated Applications	0.00	Info	Pass	**Port:** tcp/80 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:** microsoft:iis **Evidence:** CPE: microsoft:.net_framework URI: / Version: unknown **Remediation:** No remediation is required.

ASV Scan Report Vulnerability Details

168.62.224.239						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
3		Enumerated Applications	0.00	Info	Pass	**Port:** tcp/80 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:** microsoft:iis **Evidence:** CPE: microsoft:asp.net URI: / Version: 4.0.30319 **Remediation:** No remediation is required.
4		Discovered HTTP Methods	0.00	Info	Pass	**Port:** tcp/80 Requesting the allowed HTTP OPTIONS from this host shows which HTTP protocol methods are supported by its web server. Note that, in some cases, this information is not reported by the web server accurately. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** URL: http://control.peoplevine.com/ Methods: OPTIONS, TRACE, GET, HEAD, POST

ASV Scan Report Vulnerability Details

168.62.224.239						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: Review your web server configuration and ensure that only those HTTP methods required for your business operations are enabled.
5		Discovered Web Applications	0.00	Info	Pass	**Port:** tcp/80 The following web applications were discovered on the remote HTTP server. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Remediation:** No remediation is required.
6		Discovered Web Directories	0.00	Info	Pass	**Port:** tcp/80 It was possible to guess one or more directories contained in the publicly accessible path of this web server. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** URL: http://control.peoplevine.com:80/content/ HTTP Response Code: 302

ASV Scan Report Vulnerability Details

168.62.224.239						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: http://control.peoplevine.com:80/crm/ URL: http://control.peoplevine.com:80/business/ URL: http://control.peoplevine.com:80/css/ HTTP Response Code: 403 URL: http://control.peoplevine.com:80/customers/ URL: http://control.peoplevine.com:80/error/ URL: http://control.peoplevine.com:80/files/ URL: http://control.peoplevine.com:80/icons/ URL: http://control.peoplevine.com:80/images/ URL: http://control.peoplevine.com:80/img/ URL: http://control.peoplevine.com:80/js/ URL: http://control.peoplevine.com:80/pages/ URL: http://control.peoplevine.com:80/public/ URL: http://control.peoplevine.com:80/reviews/ URL: http://control.peoplevine.com:80/service/ URL: http://control.peoplevine.com:80/services/ **Remediation:** Review these directories and verify that there is no unintentional content made available to remote users.
7		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 **Application:** microsoft:iis

ASV Scan Report Vulnerability Details

168.62.224.239						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Evidence: Subject: /OU=Domain Control Validated/CN=*.peoplevine.com Issuer: /C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure Certificate Authority - G2 Certificate Chain Depth: 0 Wildcard Subject Name: *.peoplevine.com **Remediation:** Review your certificate configurations to assure that wildcard certificates are suitable for your application.
8		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

ASV Scan Report Vulnerability Details

168.62.224.239						
#	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:** microsoft:iis **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-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : AES256-SHA256 Cipher Suite: TLSv1_2 : AES256-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA **Remediation:** No remediation is necessary.
9		SSL-TLS Certificate Information	0.00	Info	Pass	**Port:** tcp/443 Information extracted from a certificate discovered on a TLS or SSL wrapped service.

ASV Scan Report Vulnerability Details

168.62.224.239						
#	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:** microsoft:iis **Evidence:** Verified: true Today: 2018-07-10 01:16:10 -0500 Start date: 2017-10-12 04:07:00 UTC End date: 2019-01-09 16:10:00 UTC Expired: false Fingerprint: 57:9C:F5:C0:95:9B:38:62:04:F9:B5:B2:27:1D:F2:97 Subject: /OU=Domain Control Validated/CN=*.peoplevine.com Common name: *.peoplevine.com Issuer: /C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certs.godaddy.com/repository//CN=Go Daddy Secure Certificate Authority - G2 Signature Algorithm: sha256WithRSAEncryption Version: 2
10		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:** microsoft:iis **Evidence:** CPE: microsoft:iis

ASV Scan Report Vulnerability Details

168.62.224.239						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URI: / Version: 10.0 **Remediation:** No remediation is required.
11		URLScan Detected	0.00	Info	Pass	**Port:** tcp/443 The web server appears to be using Microsoft's URLScan tool, an ISAPI filter that can be configured to block specified web requests. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Reference:** http://technet.microsoft.com/en-us/security/cc242650.aspx **Evidence:** Method: urlscan.ini 'MaxQueryString' is set to the default of 2048. Query strings longer than 2048 characters are rejected. **Remediation:** No remediation necessary. This is identified for informational purposes.
12		Enumerated Applications	0.00	Info	Pass	**Port:** tcp/443 The following applications have been enumerated on this device.

ASV Scan Report Vulnerability Details

168.62.224.239						
#	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:** microsoft:iis **Evidence:** CPE: microsoft:.net_framework URI: / Version: unknown **Remediation:** No remediation is required.
13		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:** microsoft:iis **Evidence:** CPE: microsoft:asp.net URI: / Version: 4.0.30319 **Remediation:** No remediation is required.

ASV Scan Report Vulnerability Details

168.62.224.239						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
14		Discovered HTTP Methods	0.00	Info	Pass	**Port:** tcp/443 Requesting the allowed HTTP OPTIONS from this host shows which HTTP protocol methods are supported by its web server. Note that, in some cases, this information is not reported by the web server accurately. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** URL: https://control.peoplevine.com/ Methods: OPTIONS, TRACE, GET, HEAD, POST **Remediation:** Review your web server configuration and ensure that only those HTTP methods required for your business operations are enabled.
15		Discovered Web Applications	0.00	Info	Pass	**Port:** tcp/443 The following web applications were discovered on the remote HTTP server. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Remediation:** No remediation is required.

ASV Scan Report Vulnerability Details

168.62.224.239						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
16		Discovered Web Directories	0.00	Info	Pass	**Port:** tcp/443 It was possible to guess one or more directories contained in the publicly accessible path of this web server. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** URL: https://control.peoplevine.com:443/content/ HTTP Response Code: 302 URL: https://control.peoplevine.com:443/crm/ URL: https://control.peoplevine.com:443/business/ URL: https://control.peoplevine.com:443/css/ HTTP Response Code: 403 URL: https://control.peoplevine.com:443/customers/ URL: https://control.peoplevine.com:443/error/ HTTP Response Code: 200 URL: https://control.peoplevine.com:443/files/ URL: https://control.peoplevine.com:443/icons/ URL: https://control.peoplevine.com:443/images/ URL: https://control.peoplevine.com:443/img/ URL: https://control.peoplevine.com:443/js/ URL: https://control.peoplevine.com:443/pages/ URL: https://control.peoplevine.com:443/public/ URL: https://control.peoplevine.com:443/reviews/ URL: https://control.peoplevine.com:443/service/

ASV Scan Report Vulnerability Details

168.62.224.239						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://control.peoplevine.com:443/services/ **Remediation:** Review these directories and verify that there is no unintentional content made available to remote users.
17		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: peoplevine.com, Source: SSL Certificate Subject subjectAltName DNS **Remediation:** No action is required.