Trustwave®

Report Date: 2020-07-23

Attestation of Scan Compliance

A.1 Scan Customer Information

Company:	HEMKO Systems Corporation		
Contact Name:	Harry Hemstreet	**Job Title:**	
Telephone:	970-667-0460	**E-mail:**	hhemstreet@hemko.com
Business Address:	5560 Stone Church Court		
City:	Loveland	**State/Province:**	Colorado
ZIP/Postal Code:	80537	**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:	2020-07-23	Scan expiration date (90 days from date scan completed):	2020-10-23
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

HEMKO Systems Corporation attests on 2020-07-23 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. HEMKO Systems Corporation 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.

	Ken Dunnington
Signature	Printed Name
Security Officer	23 JUL 2020
Title	Date

A.5 ASV Attestation

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

ASV Scan Report Summary

Part 1. Scan Information

Scan Customer Company	HEMKO Systems Corporation	ASV Company	Trustwave Holdings, Inc.
Date Scan Completed	2020-07-23	Scan Expiration Date	2020-10-21

Part 2. Component Compliance Summary

Component (IP Address, domain, etc):	67.227.238.88 - pay.planetreg.com (pay.planetreg.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	67.227.238.88 (pay.planetreg.com)	Discovered HTTP Methods	Info	0.00	Pass	
2	67.227.238.88 (pay.planetreg.com)	Discovered Web Applications	Info	0.00	Pass	
3	67.227.238.88 (pay.planetreg.com)	Discovered Web Directories	Info	0.00	Pass	**Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database.
4	67.227.238.88 (pay.planetreg.com)	Enumerated Applications	Info	0.00	Pass	**Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database.
5	67.227.238.88 (pay.planetreg.com)	Enumerated Hostnames	Info	0.00	Pass	

#	Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls (Noted by the ASV for this vulnerability)
6	67.227.238.88 (pay.planetreg.com)	Enumerated SSL/TLS Cipher Suites	Info	0.00	Pass	
7	67.227.238.88 (pay.planetreg.com)	Protected Web Page	Info	0.00	Pass	
8	67.227.238.88 (pay.planetreg.com)	SSL Certificate Expiring Soon	Info	0.00	Pass	
9	67.227.238.88 (pay.planetreg.com)	SSL-TLS Certificate Information	Info	0.00	Pass	**Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database.
10	67.227.238.88 (pay.planetreg.com)	TLSv1.1 Supported	Info	0.00	Pass	
11	67.227.238.88 (pay.planetreg.com)	TLSv1.2 Supported	Info	0.00	Pass	
12	67.227.238.88 (pay.planetreg.com)	Unknown services found	Info	0.00	Pass	
13	67.227.238.88 (pay.planetreg.com)	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.

#	Component	Vulnerabilities Noted per Component	Severity Level	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls (Noted by the ASV for this vulnerability)
• Restrict access to any files, applications, and/or network services for which there is no business requirement to be publicly accessible. • Ensure that any web applications running on this host is configured following industry security best practices.						

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
1	67.227.238.88 (pay.planetreg.com)	Unknown services	tcp/49668 generic_tcp	

Part 3c. Special Notes - Full Text

Note
Customer Note Customer has not validated that all servers behind load balancers are identical and synchronized.
Unknown services Note to scan customer: Unidentified services have been detected. Due to increased risk to the cardholder data environment, identify the service, then either 1) justify the business need for this service and confirm it is securely implemented, or 2) identify the service and confirm that it is disabled. Consult your ASV if you have questions about this Special Note.

Part 4a. Scope Submitted by Scan Customer for Discovery

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

IP Address/ranges/subnets, domains, URLs, etc.
Domain: pay.planetreg.com

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

IP Address/ranges/subnets, domains, URLs, etc.
67.227.238.88 (pay.planetreg.com)

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

IP Address/ranges/subnets, domains, URLs, etc.
No Data

Confidential Information: This document may contain information that is privileged, confidential or otherwise protected from disclosure. Dissemination, distribution or copying of this document or the information herein is prohibited without prior permission of Trustwave and HEMKO Systems Corporation .

ASV Scan Report Vulnerability Details

Part 1. Scan Information

Scan Customer Company	HEMKO Systems Corporation	ASV Company	Trustwave Holdings, Inc.
Date Scan Completed	2020-07-23	Scan Expiration Date	2020-10-21

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.

67.227.238.88 (pay.planetreg.com)

#	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

67.227.238.88 (pay.planetreg.com)						
#	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

67.227.238.88 (pay.planetreg.com)

#	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:** Methods: OPTIONS, TRACE, GET, HEAD, POST URL: http://67.227.238.88/

67.227.238.88 (pay.planetreg.com)

#	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:** HTTP Response Code: 403 URL: http://67.227.238.88:80/css/

67.227.238.88 (pay.planetreg.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						HTTP Response Code: 401 URL: http://67.227.238.88:80/reports/ **Remediation:** Review these directories and verify that there is no unintentional content made available to remote users.
7		Protected Web Page	0.00	Info	Pass	**Port:** tcp/80 The web server requires authentication for some resources. Several authentication types are available such as: 1) Basic is the most simplistic and sends credentials in clear text 2) NTLM can be used for single sign on in a Microsoft environment, but it cannot be used on both a proxy and the web server 3) Digest is a cryptographically strong scheme but credentials can still be brute forced or discovered through dictionary attacks. Note that this list is limited to ten instances of this finding. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** Authentication Type: ntlm Authentication Realm: Protected Webpage: http://67.227.238.88/reports/ **Remediation:** Confirm that the authentication in use is appropriate.

Confidential Information: This document may contain information that is privileged, confidential or otherwise protected from disclosure. Dissemination, distribution or copying of this document or the information herein is prohibited without prior permission of Trustwave and HEMKO Systems Corporation .

ASV Scan Report Vulnerability Details

67.227.238.88 (pay.planetreg.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
8		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:** Methods: OPTIONS, TRACE, GET, HEAD, POST URL: http://pay.planetreg.com/ **Remediation:** Review your web server configuration and ensure that only those HTTP methods required for your business operations are enabled.
9		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

67.227.238.88 (pay.planetreg.com)

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Evidence: HTTP Response Code: 403 URL: http://pay.planetreg.com:80/css/ HTTP Response Code: 401 URL: http://pay.planetreg.com:80/reports/ **Remediation:** Review these directories and verify that there is no unintentional content made available to remote users.
10		Protected Web Page	0.00	Info	Pass	**Port:** tcp/80 The web server requires authentication for some resources. Several authentication types are available such as: 1) Basic is the most simplistic and sends credentials in clear text 2) NTLM can be used for single sign on in a Microsoft environment, but it cannot be used on both a proxy and the web server 3) Digest is a cryptographically strong scheme but credentials can still be brute forced or discovered through dictionary attacks. Note that this list is limited to ten instances of this finding. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** Authentication Type: ntlm Authentication Realm: Protected Webpage: http://pay.planetreg.com/reports/

67.227.238.88 (pay.planetreg.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: Confirm that the authentication in use is appropriate.
11		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 **Evidence:** Subject: /CN=*.planetreg.com Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=RapidSSL RSA CA 2018 Certificate Chain Depth: 0 Wildcard Subject Name: *.planetreg.com **Remediation:** Review your certificate configurations to assure that wildcard certificates are suitable for your application.
12		SSL Certificate Expiring Soon	0.00	Info	Pass	**Port:** tcp/443 This SSL certificate is currently valid; however, it is set to expire in the near future.

67.227.238.88 (pay.planetreg.com)						
#	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:** Subject: /CN=*.planetreg.com Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=RapidSSL RSA CA 2018 Certificate Chain Depth: 0 Expiration Date: 2020-10-03 12:00:00 UTC Days to expiration: 71 **Remediation:** Contact your Certificate Authority (CA) to have a new certificate issued prior to the expiration date. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
13		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

67.227.238.88 (pay.planetreg.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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 **Application:** microsoft:iis **Reference:** http://www.openssl.org/docs/apps/ciphers.html **Evidence:** Cipher Suite: TLSv1_1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : AES256-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : AES128-SHA 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

67.227.238.88 (pay.planetreg.com)

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: No remediation is necessary.
14		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 **Application:** microsoft:iis **Evidence:** Verified: true Today: 2020-07-23 10:35:25 -0500 Start date: 2018-10-04 00:00:00 UTC End date: 2020-10-03 12:00:00 UTC Expired: false Fingerprint: 41:E4:75:01:3B:13:B8:8A:82:4E:C7:63:4C:76:0E:B2 Subject: /CN=*.planetreg.com Common name: *.planetreg.com Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=RapidSSL RSA CA 2018 Signature Algorithm: sha256WithRSAEncryption Version: 2
15		TLSv1.1 Supported	0.00	Info	Pass	**Port:** tcp/443 This service supports the use of the TLSv1.1 protocol.

67.227.238.88 (pay.planetreg.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						CVSSv2: AV:N/AC:H/Au:M/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **Evidence:** Cipher Suite: TLSv1_1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : AES256-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : AES128-SHA
16		TLSv1.2 Supported	0.00	Info	Pass	**Port:** tcp/443 This service supports the use of the TLSv1.2 protocol. **CVSSv2:** AV:N/AC:H/Au:M/C:N/I:N/A:N **Service:** http **Application:** microsoft:iis **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

67.227.238.88 (pay.planetreg.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1_2 : AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA
17		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 URI: / Version: 10.0 **Remediation:** No remediation is required.
18		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:**

67.227.238.88 (pay.planetreg.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						CPE: microsoft:.net_framework URI: / Version: unknown **Remediation:** No remediation is required.
19		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.
20		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.

ASV Scan Report Vulnerability Details

67.227.238.88 (pay.planetreg.com)						
#	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:** Methods: OPTIONS, TRACE, GET, HEAD, POST URL: https://67.227.238.88/ **Remediation:** Review your web server configuration and ensure that only those HTTP methods required for your business operations are enabled.
21		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.
22		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.

67.227.238.88 (pay.planetreg.com)

#	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:** HTTP Response Code: 403 URL: https://67.227.238.88:443/css/ **Remediation:** Review these directories and verify that there is no unintentional content made available to remote users.
23		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:** Methods: OPTIONS, TRACE, GET, HEAD, POST URL: https://pay.planetreg.com/ **Remediation:** Review your web server configuration and ensure that only those HTTP

67.227.238.88 (pay.planetreg.com)

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						methods required for your business operations are enabled.
24		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:** HTTP Response Code: 403 URL: https://pay.planetreg.com:443/css/ **Remediation:** Review these directories and verify that there is no unintentional content made available to remote users.
25		Unknown services found	0.00	Info	Pass	**Port:** tcp/49668 The finding reports all ports and protocols that couldn't be remotely identified. Particular items may indicate uncommon but safe protocols or in-house application that uses custom and/or proprietary protocol. However they can as well indicate malicious activity (backdoors, rootkits, any other types of malware). This finding is purely informational. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N

67.227.238.88 (pay.planetreg.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Service: generic_tcp **Evidence:** Unknown Service: transport protocol: tcp, port: 49668, ssl: false, banner: (N/A) **Remediation:** Review items mentioned in this finding one by one and ensure the services are known and accounted for in your security plan.
26		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: planetreg.com, Source: SSL Certificate Subject subjectAltName DNS **Remediation:** No action is required.

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:	