Trustwave®

Report Date: 2013-11-11

Vulnerability Scan Report: Attestation of Compliance

Scan Customer Information

Company Name:	Mountain Drop-Off		
Contact:	Simon Hills	Title:	
Telephone:	0033688081474	E-mail:	Simon@mountaindropoffs.com
Business Address:	Unit K, Reliance Wharf Hertford Road		
City:	London	State/Province:	London
ZIP/Postal Code:	N1 5EW	Country:	GB

Approved Scanning Vendor Information

Company Name:	Trustwave		
Contact:	Trustwave Support	URL:	www.trustwave.com
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

Scan Status

Fail	Scan Compliance Status
1	Number of unique components scanned that are in scope
7	Number of identified failing vulnerabilities
0	Number of components scanned by TrustKeeper but confirmed by the customer not to be in scope
2013-11-09	Date Scan Completed
N/A	Scan Expiration Date (3 months from Date Scan Completed)

Scan Customer Attestation

Mountain Drop-Off attests that: This scan 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 is accurate and complete. Mountain Drop-Off also acknowledges the following: 1) proper 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 the PCI DSS; This scan does not represent Mountain Drop-Offs overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

Signature

Printed Name

Title

Date

Approved Scanning Vendor Attestation

This scan and report were prepared and conducted by Trustwave under certificate number 3702-01-07 (2012), 3702-01-06 (2011), 3702-01-05 (2010), according to internal processes that meet PCI DSS requirement 11.2 and the PCI DSS 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, and 3) active interference. This report and any exceptions were reviewed by the Trustwave Quality Assurance Process.

Trustwave®

Report Date: 2013-11-11

Vulnerability Scan Report: Table of Contents

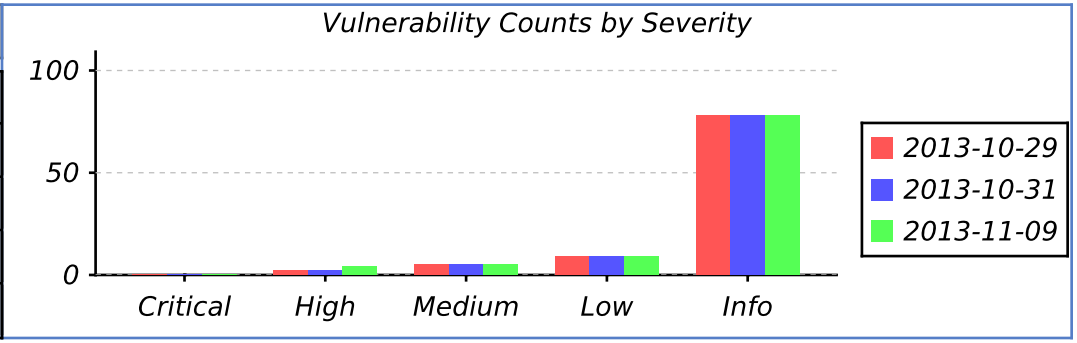
Trustwave®

Report Date: 2013-11-11

Vulnerability Scan Report: Executive Summary

Part 1. Scan Information

Scan Customer Company	Mountain Drop-Off
ASV Company	Trustwave
Scan Compliance Status	Fail
Date Scan Completed	2013-11-09
Scan Expiration Date	N/A



Part 2. Component Compliance Summary

#	Compliance Status	Name	Type	IP Address	Source	Critical	High	Medium	Low	Info
1	Fail	www.mountaindropoffs.com	Web Site	78.109.167.20	Domain Name	0	4	5	9	78
					Total Findings	**0**	**4**	**5**	**9**	**78**
					Total PCI Vulnerabilities	**0**	**2**	**5**	**0**	**0**

* Note: This location did not respond to probes from the TrustKeeper scanners. For physical locations this is good, since the location is protected and hidden from the Internet. For websites, it could mean the web site is not available, or the domain name is misspelled.

Part 3a. Vulnerabilities Noted for Each IP Address

#	IP Address	Vulnerabilities Noted	Severity	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
1	78.109.167.20	Unencrypted Communication Channel Accessibility	High	9.40	Fail	
2	78.109.167.20	Unencrypted Communication Channel Accessibility	High	9.40	Fail	
3	78.109.167.20	OpenSSH X11 Session Hijacking Vulnerability, CVE-2008-1483	Medium	6.90	Fail	
4	78.109.167.20	Reflected Cross-Site Scripting (XSS) Vulnerability	Medium	4.30	Fail	
5	78.109.167.20	Reflected Cross-Site Scripting (XSS) Vulnerability	Medium	4.30	Fail	
6	78.109.167.20	Reflected Cross-Site Scripting (XSS) Vulnerability	Medium	4.30	Fail	
7	78.109.167.20	Reflected Cross-Site Scripting (XSS) Vulnerability	Medium	4.30	Fail	
8	78.109.167.20	OpenSSH < 4.4 Multiple Vulnerabilities, CVE-2006-5051 CVE-2006-5052	High	9.30	Pass	Auto-confirming appeal by false positive analysis AUTO_CONFIRMED by false positive analysis
9	78.109.167.20	HTTP Server Overlapping Byte-Range Denial of Service, CVE-2011-3192	High	7.80	Pass	
10	78.109.167.20	OpenSSH Duplicate Block Denial of Service Vulnerability, CVE-2006-4924	High	7.80	Pass	
11	78.109.167.20	OpenSSH Privilege Separation Monitor Weakness, CVE-2006-5794	High	7.50	Pass	Auto-confirming appeal by false positive analysis AUTO_CONFIRMED by false positive

#	IP Address	Vulnerabilities Noted	Severity	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
						analysis
12	78.109.167.20	OpenSSH X11 Cookie Local Authentication Bypass Vulnerability, CVE-2007-4752	High	7.50	Pass	Auto-confirming appeal by false positive analysis AUTO_CONFIRMED by false positive analysis
13	78.109.167.20	SSLv2 Supported	Medium	5.00	Pass	Auto-confirming appeal by false positive analysis AUTO_CONFIRMED by false positive analysis
14	78.109.167.20	Indexable Web Directories	Low	2.60	Pass	
15	78.109.167.20	Indexable Web Directories	Low	2.60	Pass	
16	78.109.167.20	OpenSSH CBC Mode Information Disclosure Vulnerability, CVE-2008-5161	Low	2.60	Pass	
17	78.109.167.20	SSL Weak Encryption Algorithms	Low	1.80	Pass	
18	78.109.167.20	Auto-Completion Enabled for Password Fields	Low	1.30	Pass	
19	78.109.167.20	Auto-Completion Enabled for Password Fields	Low	1.30	Pass	
20	78.109.167.20	ProFTPD UserOwner Directive Race Condition Vulnerability, CVE-2012-6095	Low	1.20	Pass	
21	78.109.167.20	Admin Interface Detected	Low	0.00	Pass	

Vulnerability Scan Report: Executive Summary

#	IP Address	Vulnerabilities Noted	Severity	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
22	78.109.167.20	Remote Access Service Detected	Low	0.00	Pass	
23	78.109.167.20	SSHv2 Recon	Info	5.00	Pass	
24	78.109.167.20	TCP Timestamp Options Enabled	Info	0.00	Pass	
25	78.109.167.20	Enumerated Applications	Info	0.00	Pass	
26	78.109.167.20	TCP Timestamp Options Enabled	Info	0.00	Pass	
27	78.109.167.20	SMTP Service Supports the STARTTLS Command	Info	0.00	Pass	
28	78.109.167.20	OV/DV Certificate Detected	Info	0.00	Pass	
29	78.109.167.20	SSL Certificate Common Name Does Not Validate	Info	0.00	Pass	
30	78.109.167.20	SSL Certificate is Self-Signed	Info	0.00	Pass	
31	78.109.167.20	SSL Certificate is Not Trusted	Info	0.00	Pass	
32	78.109.167.20	SSL Certificate Expired	Info	0.00	Pass	
33	78.109.167.20	SSL Ephemeral Diffie-Hellman Ciphers Supported	Info	0.00	Pass	
34	78.109.167.20	Enumerated SSL/TLS Cipher Suites	Info	0.00	Pass	
35	78.109.167.20	SSL Block-based Ciphers Supported, CVE-2011-3389	Info	0.00	Pass	**NVD CVSS Score:** 2.60 **Note to scan customer:** The NVD entry for CVE-2011-3389 specifies a CVSSv2 vector of AV:N/AC:M/Au:N/C:P/I:N/A:N, with a base score of 4.3. Trustwave's assessment of the vulnerability differs since the flaw lies in the way web browsers communicate with this server and not in the server itself. As such,

#	IP Address	Vulnerabilities Noted	Severity	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
						Trustwave uses a CVSSv2 vector of AV:N/AC:L/Au:N/C:N/I:N/A:N, with a base score of 0.0, when assessing web server instances.
36	78.109.167.20	SSL RC4-based Ciphers Supported, CVE-2013-2566	Info	0.00	Pass	**NVD CVSS Score:** 2.60 **Note to scan customer:** The NVD entry for CVE-2013-2566 specifies a CVSSv2 vector of AV:N/AC:H/Au:N/C:P/I:N/A:N, with a base score of 2.6. Trustwave's assessment of the vulnerability differs since the flaw lies in the way web browsers communicate with this server and not in the server itself. As such, Trustwave uses a CVSSv2 vector of AV:N/AC:L/Au:N/C:N/I:N/A:N, with a base score of 0.0, when assessing web server instances.
37	78.109.167.20	Enumerated Applications	Info	0.00	Pass	
38	78.109.167.20	No X-FRAME-OPTIONS Header	Info	0.00	Pass	
39	78.109.167.20	Operating System Potentially Determined via Apache Requests	Info	0.00	Pass	
40	78.109.167.20	Discovered Web Directories	Info	0.00	Pass	
41	78.109.167.20	Discovered HTTP Methods	Info	0.00	Pass	
42	78.109.167.20	OV/DV Certificate Detected	Info	0.00	Pass	
43	78.109.167.20	SSL Certificate Common Name	Info	0.00	Pass	

#	IP Address	Vulnerabilities Noted	Severity	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
		Does Not Validate				
44	78.109.167.20	SSL Certificate is Self-Signed	Info	0.00	Pass	
45	78.109.167.20	SSL Certificate is Not Trusted	Info	0.00	Pass	
46	78.109.167.20	SSL Certificate Expired	Info	0.00	Pass	
47	78.109.167.20	Enumerated SSL/TLS Cipher Suites	Info	0.00	Pass	
48	78.109.167.20	SSL Block-based Ciphers Supported, CVE-2011-3389	Info	0.00	Pass	**NVD CVSS Score:** 2.60 **Note to scan customer:** The NVD entry for CVE-2011-3389 specifies a CVSSv2 vector of AV:N/AC:M/Au:N/C:P/I:N/A:N, with a base score of 4.3. Trustwave's assessment of the vulnerability differs since the flaw lies in the way web browsers communicate with this server and not in the server itself. As such, Trustwave uses a CVSSv2 vector of AV:N/AC:L/Au:N/C:N/I:N/A:N, with a base score of 0.0, when assessing web server instances.
49	78.109.167.20	SSL RC4-based Ciphers Supported, CVE-2013-2566	Info	0.00	Pass	**NVD CVSS Score:** 2.60 **Note to scan customer:** The NVD entry for CVE-2013-2566 specifies a CVSSv2 vector of AV:N/AC:H/Au:N/C:P/I:N/A:N, with a base score of 2.6. Trustwave's assessment of the vulnerability differs since the flaw lies in the way web browsers communicate with this server and

#	IP Address	Vulnerabilities Noted	Severity	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
						not in the server itself. As such, Trustwave uses a CVSSv2 vector of AV:N/AC:L/Au:N/C:N/I:N/A:N, with a base score of 0.0, when assessing web server instances.
50	78.109.167.20	IMAP Service Supports the STARTTLS Command	Info	0.00	Pass	
51	78.109.167.20	OV/DV Certificate Detected	Info	0.00	Pass	
52	78.109.167.20	SSL Certificate Common Name Does Not Validate	Info	0.00	Pass	
53	78.109.167.20	SSL Certificate is Self-Signed	Info	0.00	Pass	
54	78.109.167.20	SSL Certificate is Not Trusted	Info	0.00	Pass	
55	78.109.167.20	SSL Certificate Expired	Info	0.00	Pass	
56	78.109.167.20	Enumerated SSL/TLS Cipher Suites	Info	0.00	Pass	
57	78.109.167.20	SSL Block-based Ciphers Supported, CVE-2011-3389	Info	0.00	Pass	**NVD CVSS Score:** 2.60 **Note to scan customer:** The NVD entry for CVE-2011-3389 specifies a CVSSv2 vector of AV:N/AC:M/Au:N/C:P/I:N/A:N, with a base score of 4.3. Trustwave's assessment of the vulnerability differs since the flaw lies in the way web browsers communicate with this server and not in the server itself. As such, Trustwave uses a CVSSv2 vector of AV:N/AC:L/Au:N/C:N/I:N/A:N, with a base score of 0.0, when assessing web server instances.

#	IP Address	Vulnerabilities Noted	Severity	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
58	78.109.167.20	SSL RC4-based Ciphers Supported, CVE-2013-2566	Info	0.00	Pass	**NVD CVSS Score:** 2.60 **Note to scan customer:** The NVD entry for CVE-2013-2566 specifies a CVSSv2 vector of AV:N/AC:H/Au:N/C:P/I:N/A:N, with a base score of 2.6. Trustwave's assessment of the vulnerability differs since the flaw lies in the way web browsers communicate with this server and not in the server itself. As such, Trustwave uses a CVSSv2 vector of AV:N/AC:L/Au:N/C:N/I:N/A:N, with a base score of 0.0, when assessing web server instances.
59	78.109.167.20	OV/DV Certificate Detected	Info	0.00	Pass	
60	78.109.167.20	SSL Ephemeral Diffie-Hellman Ciphers Supported	Info	0.00	Pass	
61	78.109.167.20	Enumerated SSL/TLS Cipher Suites	Info	0.00	Pass	
62	78.109.167.20	SSL Block-based Ciphers Supported, CVE-2011-3389	Info	0.00	Pass	**NVD CVSS Score:** 2.60 **Note to scan customer:** The NVD entry for CVE-2011-3389 specifies a CVSSv2 vector of AV:N/AC:M/Au:N/C:P/I:N/A:N, with a base score of 4.3. Trustwave's assessment of the vulnerability differs since the flaw lies in the way web browsers communicate with this server and not in the server itself. As such,

#	IP Address	Vulnerabilities Noted	Severity	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
						Trustwave uses a CVSSv2 vector of AV:N/AC:L/Au:N/C:N/I:N/A:N, with a base score of 0.0, when assessing web server instances.
63	78.109.167.20	SSL RC4-based Ciphers Supported, CVE-2013-2566	Info	0.00	Pass	**NVD CVSS Score:** 2.60 **Note to scan customer:** The NVD entry for CVE-2013-2566 specifies a CVSSv2 vector of AV:N/AC:H/Au:N/C:P/I:N/A:N, with a base score of 2.6. Trustwave's assessment of the vulnerability differs since the flaw lies in the way web browsers communicate with this server and not in the server itself. As such, Trustwave uses a CVSSv2 vector of AV:N/AC:L/Au:N/C:N/I:N/A:N, with a base score of 0.0, when assessing web server instances.
64	78.109.167.20	Enumerated Applications	Info	0.00	Pass	
65	78.109.167.20	No X-FRAME-OPTIONS Header	Info	0.00	Pass	
66	78.109.167.20	Operating System Potentially Determined via Apache Requests	Info	0.00	Pass	
67	78.109.167.20	Discovered Web Directories	Info	0.00	Pass	
68	78.109.167.20	HTTP Responses Missing Character Encoding	Info	0.00	Pass	
69	78.109.167.20	HTTP Responses Missing Character Encoding	Info	0.00	Pass	

Vulnerability Scan Report: Executive Summary

#	IP Address	Vulnerabilities Noted	Severity	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
70	78.109.167.20	HTTP Responses Missing Character Encoding	Info	0.00	Pass	
71	78.109.167.20	HTTP Responses Missing Character Encoding	Info	0.00	Pass	
72	78.109.167.20	HTTP Responses Missing Character Encoding	Info	0.00	Pass	
73	78.109.167.20	HTTP Responses Missing Character Encoding	Info	0.00	Pass	
74	78.109.167.20	Web Application Potentially Sensitive CGI Parameter Detection	Info	0.00	Pass	
75	78.109.167.20	Web Application Potentially Sensitive CGI Parameter Detection	Info	0.00	Pass	
76	78.109.167.20	Web Application Potentially Sensitive CGI Parameter Detection	Info	0.00	Pass	
77	78.109.167.20	Web Application Potentially Sensitive CGI Parameter Detection	Info	0.00	Pass	
78	78.109.167.20	Discovered HTTP Methods	Info	0.00	Pass	
79	78.109.167.20	Non-HttpOnly Session Cookies Identified	Info	0.00	Pass	
80	78.109.167.20	Enumerated Applications	Info	0.00	Pass	
81	78.109.167.20	OV/DV Certificate Detected	Info	0.00	Pass	
82	78.109.167.20	SSL Certificate Common Name Does Not Validate	Info	0.00	Pass	
83	78.109.167.20	SSL Certificate is Self-Signed	Info	0.00	Pass	
84	78.109.167.20	SSL Certificate is Not Trusted	Info	0.00	Pass	
85	78.109.167.20	SSL Certificate Expired	Info	0.00	Pass	
86	78.109.167.20	SSL Ephemeral Diffie-Hellman Ciphers Supported	Info	0.00	Pass	

Vulnerability Scan Report: Executive Summary

#	IP Address	Vulnerabilities Noted	Severity	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
87	78.109.167.20	Enumerated SSL/TLS Cipher Suites	Info	0.00	Pass	
88	78.109.167.20	SSL Block-based Ciphers Supported, CVE-2011-3389	Info	0.00	Pass	**NVD CVSS Score:** 2.60 **Note to scan customer:** The NVD entry for CVE-2011-3389 specifies a CVSSv2 vector of AV:N/AC:M/Au:N/C:P/I:N/A:N, with a base score of 4.3. Trustwave's assessment of the vulnerability differs since the flaw lies in the way web browsers communicate with this server and not in the server itself. As such, Trustwave uses a CVSSv2 vector of AV:N/AC:L/Au:N/C:N/I:N/A:N, with a base score of 0.0, when assessing web server instances.
89	78.109.167.20	SSL RC4-based Ciphers Supported, CVE-2013-2566	Info	0.00	Pass	**NVD CVSS Score:** 2.60 **Note to scan customer:** The NVD entry for CVE-2013-2566 specifies a CVSSv2 vector of AV:N/AC:H/Au:N/C:P/I:N/A:N, with a base score of 2.6. Trustwave's assessment of the vulnerability differs since the flaw lies in the way web browsers communicate with this server and not in the server itself. As such, Trustwave uses a CVSSv2 vector of AV:N/AC:L/Au:N/C:N/I:N/A:N, with a base score of 0.0, when assessing web server instances.

Vulnerability Scan Report: Executive Summary

#	IP Address	Vulnerabilities Noted	Severity	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
90	78.109.167.20	No X-FRAME-OPTIONS Header	Info	0.00	Pass	
91	78.109.167.20	Enumerated Applications	Info	0.00	Pass	
92	78.109.167.20	Discovered Web Directories	Info	0.00	Pass	
93	78.109.167.20	HTTP Responses Missing Character Encoding	Info	0.00	Pass	
94	78.109.167.20	HTTP Responses Missing Character Encoding	Info	0.00	Pass	
95	78.109.167.20	HTTP Responses Missing Character Encoding	Info	0.00	Pass	
96	78.109.167.20	Web Application Potentially Sensitive CGI Parameter Detection	Info	0.00	Pass	
97	78.109.167.20	Web Application Potentially Sensitive CGI Parameter Detection	Info	0.00	Pass	
98	78.109.167.20	Discovered HTTP Methods	Info	0.00	Pass	
99	78.109.167.20	Discovered Web Applications	Info	0.00	Pass	
100	78.109.167.20	POP3 Service Supports the STARTTLS Command	Info		Pass	

Consolidated Solution/Correction Plan for the above IP Address:

- Configure the HTTP service(s) running on this host to adhere to information security best practices.
- Configure the SSH service(s) running on this host to adhere to information security best practices.
- Configure the SSL service(s) running on this host to adhere to information security best practices.
- Upgrade and/or install security updates for Apache HTTP Server.
- Upgrade and/or install security updates for OpenSSH.
- Upgrade and/or install security updates for ProFTPD.
- Ensure that any web applications running on this host properly validate and transmit user input in a secure manner.

Part 3b. Special Notes by IP Address

#	IP Address	Note	Item Noted (remote access software, POS software, etc.)	Scan customer's declaration that software is implemented securely (see next column if not implemented securely)	Scan customer's description of actions taken to either: 1) remove the software or 2) implement security controls to secure the software
1	78.109.167.20	**Directory Browsing Enabled** Note to scan customer: Browsing of directories on web servers can lead to information disclosure or potential exploit. Due to increased risk to the cardholder data environment, please 1) justify the business need for this configuration to the ASV, or 2) confirm that it is disabled. Please consult your ASV if you have questions about this Special Note.	tcp/80 http (apache: http_server)		
2	78.109.167.20	**Directory Browsing Enabled** Note to scan customer: Browsing of directories on web servers can lead to information disclosure or potential exploit. Due to increased risk to the cardholder data environment, please 1) justify the business need for this configuration to the ASV, or 2) confirm that it is disabled. Please consult your ASV if you have questions about this Special Note.	tcp/443 http (apache: http_server)		
3	78.109.167.20	**Remote Access Detected** Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix C or disabled/ removed. Please	tcp/2020 ssh (openssh: openssh)		

#	IP Address	Note	Item Noted (remote access software, POS software, etc.)	Scan customer's declaration that software is implemented securely (see next column if not implemented securely)	Scan customer's description of actions taken to either: 1) remove the software or 2) implement security controls to secure the software
		consult your ASV if you have questions about this Special Note.			
4	78.109.167.20	**Remote Access Detected** Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix C or disabled/ removed. Please consult your ASV if you have questions about this Special Note.	tcp/8443 http		

Vulnerability Scan Report: Vulnerability Details

Part 1. Scan Information

Scan Customer Company	Mountain Drop-Off	Data Scan Completed	2013-11-09
ASV Company	Trustwave	Scan Expiration Date	N/A

Part 2. Scan Inventory (Accessible Systems and Services)

The following systems and network services were detected during this scan. This information is provided for your information. Please refer to "Part 4. Vulnerabilities & Policy Violations" for all PCI compliance-related issues.

Reading Your Scan Inventory

The vulnerability scan reveals Internet-accessible computers and network services available on your network. The following systems (e.g., computers, servers, routers, etc.) and network services (e.g., Web and mail servers) were discovered during the vulnerability scan. As a general rule, all unnecessary network services should be disabled, and all other services should be protected by a firewall or similar device. Only those services which must be available to the public should be visible from the Internet.

- *Names* - A system may be known by many names. For example, a server that offers Web and mail services may be known as both www.mycompany.com and mail.mycompany.com. This report includes as many names as could be identified, including public domain names, Windows domain/workgroups, Windows name, and the "real" name assigned in your DNS server.
- *Ping* - One technique TrustKeeper uses is to try to "ping" systems in your network. It is generally considered to be good practice to block inbound pings as it can give attackers information about your network. However, this decision may be affected by network monitoring needs and other considerations.
- *Service Information* - A large number of services (e.g., TCP and UDP ports) are probed during the scan. Any that appear to be active on the device are listed in the table. You should review this list to ensure that only those services you intend to offer to the public are accessible. All other internal services should be protected by your firewall or similar device.

#	Device	Names	OS	Ping	Service Information			
					Port	Protocol	Application	Detail
1	78.109.167.20	mailserv.mountaindropoffs.com	Linux Kernel	false	tcp/21	ftp	proftpd:proftpd	220 ProFTPD 1.3.4a Server (ProFTPD) [78.109.167.20]

Vulnerability Scan Report: Vulnerability Details

#	Device	Names	OS	Ping	Service Information			
					Port	Protocol	Application	Detail
					tcp/25	smtp		220 mailserv.mountaindropoffs.com ESMTP
					tcp/80	http	apache: http_server	Apache
					tcp/110	pop3		+OK Hello there. <22563.1383985541@localhost.localdomain>
					tcp/143	imap		* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA AUTH=CRAM-MD5 IDLE ACL ACL2=UNION STARTTLS]
					tcp/443	http	apache: http_server	Apache
					tcp/2020	ssh	openssh: openssh	OpenSSH_4.3
					tcp/8443	http		sw-cp-server

#	Device	Names	OS	Ping	Service Information			
					Port	Protocol	Application	Detail
					All other scanned ports were filtered.			

Part 3a. Previous Scan Targets (Not Scanned)

The following locations were removed from your scan setup at your request and have not been included in this scan. You confirmed that these locations or domain names do not store, process, or transmit cardholder data and therefore not required to be scanned for PCI DSS compliance.

#	Name	Type	IP Address	Date Removed
No such scan locations have been removed by this customer.				

Part 3b. Discovered Scan Targets (Not Scanned)

The following systems were discovered to be related to your network during this scan. TrustKeeper only scans those systems which are explicitly identified by you; however, the following systems were identified using reconnaissance techniques based on the information you provided. While not scanned for this assessment, you should be aware that an attacker could identify the same information.

Please review this information and update your TrustKeeper Scan Setup if any of the following systems are relevant to the assessment being performed. In many cases, some of these systems will not be relevant to the assessment. Common examples include domain name servers (DNS) and mail servers maintained by your ISP. The scanner may also identify internal systems that are not directly accessible from the Internet.

#	IP Address	Domain Name	Comments
1	157.56.81.41	ns2.bdm.microsoftonline.com	Discovered hosts using second-level domain name(s): mountaindropoffs.com
2	207.46.15.59	ns1.bdm.microsoftonline.com	Discovered hosts using second-level domain name(s): mountaindropoffs.com
3	213.199.154.23	mountaindropoffs-com.mail.protection.outlook.com	Discovered hosts using second-level domain name(s): mountaindropoffs.com

Part 3c. Load Balancers

If you are using load balancers for your web sites to spread the web traffic across multiple servers, **it is your responsibility** to ensure that the configuration of the environment behind your load balancers is synchronized, or to ensure that the environment is scanned as part of the internal vulnerability scans required by PCI DSS.

Part 4. Vulnerabilities & Policy Violations

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.

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
1		Unencrypted Communication Channel Accessibility	9.40	High	Fail	**Policy Violation** **Port:** tcp/25 The service running on this port (most often Telnet, FTP, etc…) appears to make use of a plaintext (unencrypted) communication channel. Payment industry policies (PCI 1.1.5.b, 2.2.2.b, 2.3, &

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						8.4.a) forbid the use of such insecure services/protocols. Unencrypted communication channels are vulnerable to the disclosure and/or modification of any data transiting through them (including usernames and passwords), and as such the confidentially and integrity of the data in transit cannot be ensured with any level of certainty. **CVSSv2:** AV:N/AC:L/Au:N/C:C/I:C/A:N **Service:** smtp **Evidence:** Details: Unencrypted authentication is allowed prior to TLS negotiation Plaintext methods allowed: LOGIN **Remediation:** Transition to using more secure alternatives such as SSH instead of Telnet and SFTP in favor of FTP, or consider wrapping less secure services within more secure technologies by utilizing the benefits offered by VPN, SSL/TLS, or IPSec for example. Also, limit access to management protocols/services to specific IP addresses (usually accomplished via a “whitelist”) whenever possible.
2		Unencrypted Communication Channel Accessibility	9.40	High	Fail	**Policy Violation** **Port:** tcp/143 The service running on this port (most often Telnet, FTP, etc…) appears to make use of a plaintext (unencrypted) communication channel. Payment industry policies (PCI 1.1.5.b, 2.2.2.b, 2.3, & 8.4.a) forbid the use of such insecure services/protocols. Unencrypted communication channels are vulnerable to the

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						disclosure and/or modification of any data transiting through them (including usernames and passwords), and as such the confidentially and integrity of the data in transit cannot be ensured with any level of certainty. **CVSSv2:** AV:N/AC:L/Au:N/C:C/I:C/A:N **Service:** imap **Evidence:** Details: Authentication is allowed without an encrypted connection Sent: A001 LOGIN Rjuc2CE7 Xl8CDXGB Received: A001 NO PLAIN text authentication does not support **Remediation:** Transition to using more secure alternatives such as SSH instead of Telnet and SFTP in favor of FTP, or consider wrapping less secure services within more secure technologies by utilizing the benefits offered by VPN, SSL/TLS, or IPSec for example. Also, limit access to management protocols/services to specific IP addresses (usually accomplished via a “whitelist”) whenever possible.
3	CVE-2008-1483	OpenSSH X11 Session Hijacking Vulnerability	6.90	Medium	Fail	**Port:** tcp/2020 OpenSSH is prone to a vulnerability that allows local attackers to hijack forwarded X connections. The system must have both IPv4 and IPv6 enabled at the same time for this to be exploited. Successfully exploiting this issue may allow an attacker run arbitrary shell commands with the privileges of the user running the affected application. This issue is known to affect OpenSSH 4.3p2, though other versions may also be affected. This

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						vulnerability will trigger on any SSH banner version prior to 'openssh-5'. OpenSSH packages shipped with Red Hat Enterprise Linux 4 and 5 are not vulnerable to this issue. However, Red Hat Enterprise Linux 2.1 and 3 are affected. This finding is based on version information which may not have been updated by previously installed patches (e.g., Red Hat "back ports"). Please submit a "Patched Service" dispute in TrustKeeper if this vulnerability has already been patched. **CVE:** CVE-2008-1483 **NVD:** CVE-2008-1483 **Bugtraq:** 28444 **CVSSv2:** AV:L/AC:M/Au:N/C:C/I:C/A:C **Service:** ssh **Evidence:** Match: '4.3' is less than '5.0' **Remediation:** Due to the fact that this vulnerability is detected by analyzing the SSH banner version, an appeal must be submitted after following any remediation step other than upgrading to OpenSSH 5.0. There are several options for removing this issue: 1) Instruct OpenSSH to use only IPv4 *or* IPv6 by adding either "AddressFamily inet" or "AddressFamily inet6" to sshd_config. 2) Configure the operating system to only use IPv4 *or* IPv6, but not both. 3) Confirm with your vendor that your version of SSH is patched or CVE-2008-1483. 4) Upgrade to version 5.0 of OpenSSH, or acquire appropriate patches from your vendor. It is strongly recommended that the latest stable version with all of the appropriate patches be installed. 5) Disable X11 forwarding in the

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						sshd_config if it is not needed.
4		Reflected Cross-Site Scripting (XSS) Vulnerability	4.30	Medium	Fail	**Port:** tcp/443 A reflected cross-site scripting vulnerability was identified in this web application. Reflected cross-site scripting is when HTML or Javascript content is supplied to a user defined parameter to have it then displayed (aka: reflected) back to the user and rendered or interpreted by their browser. This web site responded to a harmless web request that included Javascript/HTML which was reflected back, indicating that the underlying web application may be vulnerable to being used in a cross-site scripting (XSS) attack. While this vulnerability does not exploit the web server itself, it can be utilized by an attacker to target end-users and potentially take over their sessions or other sensitive information. A simple proof of concept example of this would be for a user to supply "<script>alert('123')</script>" to a user defined parameter and then upon submission, a message box would pop-up for the user because the user defined content was used to modify the content of the responding page. Cross-site scripting can be found in many different forms and combinations so the full request and response that was used demonstrate this vulnerability has been provided below as evidence. All Cross-Site Scripting vulnerabilities are considered non-compliant by PCI.

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						CVSSv2: AV:N/AC:M/Au:N/C:N/I:P/A:N **Service:** http **Reference:** http://www.cert.org/advisories/CA-2000-02.html http://www.owasp.org/index.php/Cross-site_scripting http://www.owasp.org/index.php/Data_Validation http://www.owasp.org/index.php/Review_Code_for_Cross-site_scripting **Evidence:** URL: https://www.mountaindropoffs.com/en/login/ Parameter: N/A Request: GET /en/login/?<script>alert('TK00000031')</script> HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Host: www.mountaindropoffs.com Response: HTTP/1.1 200 OK Date: Sat, 09 Nov 2013 09:04:23 GMT Server: Apache Set-Cookie: PHPSESSID=8i1gkukid830pt18v2e21niuo5; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache P3P: CP="IDC CUR ADM OUR STP UNI" X-Powered-By: PleskLin MS-Author-Via: DAV Connection: close

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Transfer-Encoding: chunked Content-Type: text/html Evidence: <script>alert('TK00000031')</script> **Remediation:** Before accepting any user-supplied data, the application should validate this data's format and reject any characters that are not explicitly allowed (i.e. a white-list). This list should be as restrictive as possible. Before using any data (stored or user-supplied) to generate web page content, the application should escape all non alpha-numeric characters (i.e. output-validation). This is particularly important when the original source of data is beyond the control of the application. Even if the source of the data isn't performing input-validation, output-validation will still prevent XSS. Please note that the listing of XSS vulnerabilities is not an exhaustive list, and other XSS vulnerabilities may exist in the application. An application review should be performed in order to comply with PCI DSS Section 6.6. Additionally, a web application firewall (WAF) may also satisfy PCI DSS Section 6.6, however, it may still result in a failing scan.
5		Reflected Cross-Site Scripting (XSS) Vulnerability	4.30	Medium	Fail	**Port:** tcp/443 A reflected cross-site scripting vulnerability was identified in this web application. Reflected cross-site scripting is when HTML or Javascript content is supplied to a user defined parameter to have it then displayed (aka: reflected) back to the user and rendered or interpreted by their browser. This web site responded to a harmless web request that included

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Javascript/HTML which was reflected back, indicating that the underlying web application may be vulnerable to being used in a cross-site scripting (XSS) attack. While this vulnerability does not exploit the web server itself, it can be utilized by an attacker to target end-users and potentially take over their sessions or other sensitive information. A simple proof of concept example of this would be for a user to supply "<script>alert('123')</script>" to a user defined parameter and then upon submission, a message box would pop-up for the user because the user defined content was used to modify the content of the responding page. Cross-site scripting can be found in many different forms and combinations so the full request and response that was used demonstrate this vulnerability has been provided below as evidence. All Cross-Site Scripting vulnerabilities are considered non-compliant by PCI. **CVSSv2:** AV:N/AC:M/Au:N/C:N/I:P/A:N **Service:** http **Reference:** http://www.cert.org/advisories/CA-2000-02.html http://www.owasp.org/index.php/Cross-site_scripting http://www.owasp.org/index.php/Data_Validation http://www.owasp.org/index.php/Review_Code_for_Cross-site_scripting **Evidence:**

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://www.mountaindropoffs.com/en/contact-details Parameter: N/A Request: GET /en/contact-details?<script>alert('TK0000004D')</script> HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Host: www.mountaindropoffs.com Response: HTTP/1.1 200 OK Date: Sat, 09 Nov 2013 09:04:39 GMT Server: Apache Set-Cookie: PHPSESSID=vsnpj4achr0bkblv1ali4n29m3; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache P3P: CP="IDC CUR ADM OUR STP UNI" X-Powered-By: PleskLin MS-Author-Via: DAV Connection: close Transfer-Encoding: chunked Content-Type: text/html Evidence: <script>alert('TK0000004D')</script> **Remediation:** Before accepting any user-supplied data, the application should validate this data's format and reject any characters that are not explicitly allowed (i.e. a white-list). This list should be as restrictive as possible. Before using any data (stored or user-supplied) to generate web page content, the application should escape all non alpha-numeric characters (i.e. output-validation).

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						This is particularly important when the original source of data is beyond the control of the application. Even if the source of the data isn't performing input-validation, output-validation will still prevent XSS. Please note that the listing of XSS vulnerabilities is not an exhaustive list, and other XSS vulnerabilities may exist in the application. An application review should be performed in order to comply with PCI DSS Section 6.6. Additionally, a web application firewall (WAF) may also satisfy PCI DSS Section 6.6, however, it may still result in a failing scan.
6		Reflected Cross-Site Scripting (XSS) Vulnerability	4.30	Medium	Fail	**Port:** tcp/443 A reflected cross-site scripting vulnerability was identified in this web application. Reflected cross-site scripting is when HTML or Javascript content is supplied to a user defined parameter to have it then displayed (aka: reflected) back to the user and rendered or interpreted by their browser. This web site responded to a harmless web request that included Javascript/HTML which was reflected back, indicating that the underlying web application may be vulnerable to being used in a cross-site scripting (XSS) attack. While this vulnerability does not exploit the web server itself, it can be utilized by an attacker to target end-users and potentially take over their sessions or other sensitive information. A simple proof of concept example of this would be for a user to supply "<script>alert('123')</script>" to a user defined parameter and then upon submission, a message box would pop-up for the user because the user defined content was used to

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						modify the content of the responding page. Cross-site scripting can be found in many different forms and combinations so the full request and response that was used demonstrate this vulnerability has been provided below as evidence. All Cross-Site Scripting vulnerabilities are considered non-compliant by PCI. **CVSSv2:** AV:N/AC:M/Au:N/C:N/I:P/A:N **Service:** http **Reference:** http://www.cert.org/advisories/CA-2000-02.html http://www.owasp.org/index.php/Cross-site_scripting http://www.owasp.org/index.php/Data_Validation http://www.owasp.org/index.php/Review_Code_for_Cross-site_scripting **Evidence:** URL: https://www.mountaindropoffs.com/fr/login/ Parameter: N/A Request: GET /fr/login/?<script>alert('TK00000191')</script> HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Host: www.mountaindropoffs.com Response: HTTP/1.1 200 OK

Vulnerability Scan Report: Vulnerability Details

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Date: Sat, 09 Nov 2013 09:06:34 GMT Server: Apache Set-Cookie: PHPSESSID=f20tgmdj3r5stm9ougr0l75p71; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache P3P: CP="IDC CUR ADM OUR STP UNI" X-Powered-By: PleskLin MS-Author-Via: DAV Connection: close Transfer-Encoding: chunked Content-Type: text/html Evidence: <script>alert('TK00000191')</script> **Remediation:** Before accepting any user-supplied data, the application should validate this data's format and reject any characters that are not explicitly allowed (i.e. a white-list). This list should be as restrictive as possible. Before using any data (stored or user-supplied) to generate web page content, the application should escape all non alpha-numeric characters (i.e. output-validation). This is particularly important when the original source of data is beyond the control of the application. Even if the source of the data isn't performing input-validation, output-validation will still prevent XSS. Please note that the listing of XSS vulnerabilities is not an exhaustive list, and other XSS vulnerabilities may exist in the application. An application review should be performed in order to comply with PCI DSS Section 6.6. Additionally, a web application firewall (WAF) may also satisfy PCI DSS Section 6.6, however, it may still result in a failing scan.

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
7		Reflected Cross-Site Scripting (XSS) Vulnerability	4.30	Medium	Fail	**Port:** tcp/443 A reflected cross-site scripting vulnerability was identified in this web application. Reflected cross-site scripting is when HTML or Javascript content is supplied to a user defined parameter to have it then displayed (aka: reflected) back to the user and rendered or interpreted by their browser. This web site responded to a harmless web request that included Javascript/HTML which was reflected back, indicating that the underlying web application may be vulnerable to being used in a cross-site scripting (XSS) attack. While this vulnerability does not exploit the web server itself, it can be utilized by an attacker to target end-users and potentially take over their sessions or other sensitive information. A simple proof of concept example of this would be for a user to supply "<script>alert('123')</script>" to a user defined parameter and then upon submission, a message box would pop-up for the user because the user defined content was used to modify the content of the responding page. Cross-site scripting can be found in many different forms and combinations so the full request and response that was used demonstrate this vulnerability has been provided below as evidence. All Cross-Site Scripting vulnerabilities are considered non-compliant by PCI. **CVSSv2:** AV:N/AC:M/Au:N/C:N/I:P/A:N

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Service: http **Reference:** http://www.cert.org/advisories/CA-2000-02.html http://www.owasp.org/index.php/Cross-site_scripting http://www.owasp.org/index.php/Data_Validation http://www.owasp.org/index.php/Review_Code_for_Cross-site_scripting **Evidence:** URL: https://www.mountaindropoffs.com/fr/contactez_nous Parameter: N/A Request: GET /fr/contactez_nous?<script>alert('TK000001B1')</script> HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Host: www.mountaindropoffs.com Response: HTTP/1.1 200 OK Date: Sat, 09 Nov 2013 09:06:48 GMT Server: Apache Set-Cookie: PHPSESSID=6ist6hc8les7ell56bu07gcsu6; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache P3P: CP="IDC CUR ADM OUR STP UNI" X-Powered-By: PleskLin MS-Author-Via: DAV Connection: close Transfer-Encoding: chunked

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Content-Type: text/html Evidence: <script>alert('TK000001B1')</script> **Remediation:** Before accepting any user-supplied data, the application should validate this data's format and reject any characters that are not explicitly allowed (i.e. a white-list). This list should be as restrictive as possible. Before using any data (stored or user-supplied) to generate web page content, the application should escape all non alpha-numeric characters (i.e. output-validation). This is particularly important when the original source of data is beyond the control of the application. Even if the source of the data isn't performing input-validation, output-validation will still prevent XSS. Please note that the listing of XSS vulnerabilities is not an exhaustive list, and other XSS vulnerabilities may exist in the application. An application review should be performed in order to comply with PCI DSS Section 6.6. Additionally, a web application firewall (WAF) may also satisfy PCI DSS Section 6.6, however, it may still result in a failing scan.
8	CVE-2011-3192	HTTP Server Overlapping Byte-Range Denial of Service	7.80	High	Pass	**Port:** tcp/443 The remote HTTP Server responded to an HTTP request in a way that indicates that it is likely vulnerable to a Denial of Service attack. The attack sends malicious HTTP Range Request header data. The Range header is normally used when a client is requesting larger files from a web site. These files are too large to fit within the body of a single response so they are segmented and sent to

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						the client in chunks. When sending responses to range requests, web server should trigger a 206 Partial Content HTTP status code. By sending this single request with such a large number of fields within the Range header, the attacker is amplifying their request as each byte range field forces the HTTP server to make separate copies of the requested resource server-side which is consuming resources deep within the Apache internals, resulting in a denial of service. Vulnerabilities which result only in denial of service do not affect PCI compliance; however, they may still be critical to your systems. **CVE:** CVE-2011-3192 **NVD:** CVE-2011-3192 **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:C **Service:** http **Reference:** http://tools.ietf.org/html/rfc2616#section-14.35 http://blog.spiderlabs.com/2011/08/mitigation-of-apache-range-header-dos-attack.html http://mail-archives.apache.org/mod_mbox/httpd-announce/201108.mbox/%3C20110826103531.998348F82@minotaur.apache.org%3E **Evidence:** Status: 206 - Partial Content URL: https://www.mountaindropoffs.com/admin/javascript/jquery/jquery-1.4.2.js

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: Please see your HTTP Server vendor for any applicable patches. Apache HTTP Server version 2.2.20 addresses this issue, though many vendors (Redhat, Debian, etc) have also backported fixes to address the problem. It is recommended that you check with your vendor for patches. There are many avenues for mitigating the issue: using mod_rewrite to limit the number of ranges; disabling support for 'Range', or patching the source code. One other mechanism to mention is utilizing a web-application firewall, such as mod_security, to filter incoming requests (see the SpiderLabs blog for a writeup on how to mod_security may be used to mitigate this attack).
9	CVE-2006-4924	OpenSSH Duplicate Block Denial of Service Vulnerability	7.80	High	Pass	**Port:** tcp/2020 A version of OpenSSH prior to 4.4 is running on this host. This version is affected by a Denial of Service vulnerability. However, an attack can only be performed if version 1 of the SSH protocol is enabled. Vulnerabilities which result only in denial of service do not affect PCI compliance; however, they may still be critical to your systems. This finding is based on version information which may not have been updated by previously installed patches (e.g., Red Hat "back ports"). Please submit a "Patched Service" dispute in TrustKeeper if this vulnerability has already been patched.

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						CVE: CVE-2006-4924 **NVD:** CVE-2006-4924 **Bugtraq:** 20216 **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:C **Service:** ssh **Evidence:** Match: '4.3' is less than '4.4' **Remediation:** SSH version 1 should be disabled, as it has inherent weaknesses that can be leveraged for man-in-the-middle attacks.
10		Indexable Web Directories	2.60	Low	Pass	**Port:** tcp/80 One or more directories on this web server appear to allow remote users to view the directory structure and potentially navigate to sensitive data. **CVSSv2:** AV:N/AC:H/Au:N/C:P/I:N/A:N **Service:** http **Evidence:** URL: http://www.mountaindropoffs.com:80/icons/ URL: http://www.mountaindropoffs.com/icons/?C=N;O=D URL: http://www.mountaindropoffs.com/icons/?C=M;O=A URL: http://www.mountaindropoffs.com/icons/?C=S;

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: O=A URL: http://www.mountaindropoffs.com/icons/?C=D;O=A URL: http://www.mountaindropoffs.com/icons/small/ URL: http://www.mountaindropoffs.com/icons/?C=N;O=A URL: http://www.mountaindropoffs.com/icons/?C=M;O=D URL: http://www.mountaindropoffs.com/icons/?C=S;O=D URL: http://www.mountaindropoffs.com/icons/?C=D;O=D URL: http://www.mountaindropoffs.com/icons/small/?C=N;O=D URL: http://www.mountaindropoffs.com/icons/small/?C=M;O=A URL: http://www.mountaindropoffs.com/icons/small/?C=S;O=A URL: http://www.mountaindropoffs.com/icons/small/?C=D;O=A URL: http://www.mountaindropoffs.com/icons/small/?C=N;O=A URL: http://www.mountaindropoffs.com/icons/small/?C=M;O=D URL: http://www.mountaindropoffs.com/icons/small/?C=S;O=D URL: http://www.mountaindropoffs.com/icons/small/?C=D;O=D **Remediation:** Ensure that directory indexing is not enabled on this web server.

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
11		Indexable Web Directories	2.60	Low	Pass	**Port:** tcp/443 One or more directories on this web server appear to allow remote users to view the directory structure and potentially navigate to sensitive data. **CVSSv2:** AV:N/AC:H/Au:N/C:P/I:N/A:N **Service:** http **Evidence:** URL: https://www.mountaindropoffs.com:443/icons/ URL: https://www.mountaindropoffs.com/icons/?C=N;O=D URL: https://www.mountaindropoffs.com/icons/?C=M;O=A URL: https://www.mountaindropoffs.com/icons/?C=S;O=A URL: https://www.mountaindropoffs.com/icons/?C=D;O=A URL: https://www.mountaindropoffs.com/icons/small/ URL: https://www.mountaindropoffs.com/icons/?C=N;O=A URL: https://www.mountaindropoffs.com/icons/?C=M;O=D URL: https://www.mountaindropoffs.com/icons/?C=S;O=D URL: https://www.mountaindropoffs.com/icons/?C=D;O=D URL: https://www.mountaindropoffs.com/icons/small/?

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: C=N;O=D URL: https://www.mountaindropoffs.com/icons/small/?C=M;O=A URL: https://www.mountaindropoffs.com/icons/small/?C=S;O=A URL: https://www.mountaindropoffs.com/icons/small/?C=D;O=A URL: https://www.mountaindropoffs.com/icons/small/?C=N;O=A URL: https://www.mountaindropoffs.com/icons/small/?C=M;O=D URL: https://www.mountaindropoffs.com/icons/small/?C=S;O=D URL: https://www.mountaindropoffs.com/icons/small/?C=D;O=D **Remediation:** Ensure that directory indexing is not enabled on this web server.
12	CVE-2008-5161	OpenSSH CBC Mode Information Disclosure Vulnerability	2.60	Low	Pass	**Port:** tcp/2020 The detected version of OpenSSH is prone to an information-disclosure vulnerability. Successful exploits could allow attackers to obtain up to four bytes of plaintext data from an encrypted session. Versions prior to OpenSSH 5.2 are reported to be vulnerable as well as various versions of SSH Tectia. This finding is based on version information which may not have been updated by previously installed patches (e.g., Red Hat "back ports"). Please submit a "Patched Service" dispute in TrustKeeper if this vulnerability has already been patched.

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						CVE: CVE-2008-5161 **NVD:** CVE-2008-5161 **Bugtraq:** 32319 **CVSSv2:** AV:N/AC:H/Au:N/C:P/I:N/A:N **Service:** ssh **Evidence:** Match: '4.3' is greater than or equal to '4.0' Match: '4.3' is less than or equal to '5.1' **Remediation:** The Vendor has released updates that address this issue. Upgrade to the most recent current version.
13		SSL Weak Encryption Algorithms	1.80	Low	Pass	**Port:** tcp/25 The SSL-based service running on this host appears to support the use of "weak" ciphers, which are those that have key-lengths of less than 128 bits. **CVSSv2:** AV:A/AC:H/Au:N/C:P/I:N/A:N **Service:** smtp **Reference:** http://www.schneier.com/paper-ssl.pdf **Evidence:** Cipher Suite: SSLv2 : DES-CBC-MD5 Cipher Suite: SSLv2 : EXP-RC2-CBC-MD5

Vulnerability Scan Report: Vulnerability Details

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: SSLv2 : EXP-RC4-MD5 Cipher Suite: SSLv3 : EDH-RSA-DES-CBC-SHA Cipher Suite: SSLv3 : EXP-EDH-RSA-DES-CBC-SHA Cipher Suite: SSLv3 : DES-CBC-SHA Cipher Suite: SSLv3 : EXP-DES-CBC-SHA Cipher Suite: SSLv3 : EXP-RC2-CBC-MD5 Cipher Suite: SSLv3 : EXP-RC4-MD5 Cipher Suite: TLSv1 : EDH-RSA-DES-CBC-SHA Cipher Suite: TLSv1 : EXP-EDH-RSA-DES-CBC-SHA Cipher Suite: TLSv1 : DES-CBC-SHA Cipher Suite: TLSv1 : EXP-DES-CBC-SHA Cipher Suite: TLSv1 : EXP-RC2-CBC-MD5 Cipher Suite: TLSv1 : EXP-RC4-MD5 **Remediation:** Configure your SSL server to only use higher-grade encryption. OpenSSL servers classify encryption algorithms as HIGH, MEDIUM, LOW, and EXPORT strength. Algorithms classified as HIGH all use 128-bit encryption or higher, as do several that are classified as MEDIUM. The "SSLCipherSuite" configuration item for mod_ssl and Apache2 can be used to control encryption algorithms for web servers that use OpenSSL. Since the definition of HIGH, MEDIUM, LOW, and EXPORT can vary between each version of OpenSSL, it is recommended that the following be used to give the best guarantee for strong encryption: SSLCipherSuite HIGH:!SSLv2:!ADH:!aNULL:!eNULL:!NULL

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						For Windows systems running Internet Information Server (IIS), refer to the following Knowledge Base article for disabling certain cryptographic algorithms and protocols: http://support.microsoft.com/kb/245030. **Patches:** http://support.microsoft.com/kb/245030 http://httpd.apache.org/docs/2.2/ssl/
14		Auto-Completion Enabled for Password Fields	1.30	Low	Pass	**Port:** tcp/443 The web server running on this host uses password fields that allow auto-completion by users' browsers. This could allow a user's credentials to be stored by the browser and subsequently exposed if the user's computer becomes compromised. **CVSSv2:** AV:L/AC:H/Au:N/C:P/I:N/A:N **Service:** http **Reference:** http://msdn.microsoft.com/en-us/library/ms533032.aspx https://developer.mozilla.org/En/How_to_Turn_Off_Form_Autocompletion **Evidence:** Location: https://www.mountaindropoffs.com/en/login/ Form Name: (no name) Action: https://www.mountaindropoffs.com/en/login/ Fields: password (password)

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: Modify the identified page so that the password field and the enclosing form tags have an attribute named "autocomplete" with a value of "off". If this is a vendor application, contact the vendor for an updated version of the application or guidance on addressing this issue.
15		Auto-Completion Enabled for Password Fields	1.30	Low	Pass	**Port:** tcp/443 The web server running on this host uses password fields that allow auto-completion by users' browsers. This could allow a user's credentials to be stored by the browser and subsequently exposed if the user's computer becomes compromised. **CVSSv2:** AV:L/AC:H/Au:N/C:P/I:N/A:N **Service:** http **Reference:** http://msdn.microsoft.com/en-us/library/ms533032.aspx https://developer.mozilla.org/En/How_to_Turn_Off_Form_Autocompletion **Evidence:** Location: https://www.mountaindropoffs.com/fr/login/ Form Name: (no name) Action: https://www.mountaindropoffs.com/fr/login/ Fields: password (password) **Remediation:**

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Modify the identified page so that the password field and the enclosing form tags have an attribute named "autocomplete" with a value of "off". If this is a vendor application, contact the vendor for an updated version of the application or guidance on addressing this issue.
16	CVE-2012-6095	ProFTPD UserOwner Directive Race Condition Vulnerability	1.20	Low	Pass	**Port:** tcp/21 ProFTPD before 1.3.5rc1, when using the UserOwner directive, allows local users to modify the ownership of arbitrary files via a race condition and a symlink attack on either MKD or XMKD commands. This finding is based on version information which may not have been updated by previously installed patches (e.g., Red Hat "back ports"). Please submit a "Patched Service" dispute in TrustKeeper if this vulnerability has already been patched. **CVE:** CVE-2012-6095 **NVD:** CVE-2012-6095 **CVSSv2:** AV:L/AC:H/Au:N/C:N/I:P/A:N **Service:** ftp **Reference:** http://bugs.proftpd.org/show_bug.cgi?id=3841 https://github.com/Castaglia/proftpd-mod_vroot/issues/1 **Evidence:** Match: '1.3.4a' is greater than or equal to '1.3.0' Match: '1.3.4a' is less than '1.3.5rc1'

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: At the time of this writing, a patch has not been produced by the vendor. However, a work-around exists which suggests using a relative path to the chrooted path when using the <Directory> directive.
17		Admin Interface Detected	0.00	Low	Pass	**Port:** tcp/8443 An administrative interface is accessible on the remote host. This interface can be used to manage system settings and/or services. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Evidence:** Name: parallels:parallels_plesk_panel URL: https://www.mountaindropoffs.com:8443/ **Remediation:** Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer). Allow connections only from specific (known) IP/MAC addresses. Use strong authentication, including unique and complex passwords for logins according to PCI DSS Requirements 8.1 - 8.4 and 8.5.8 - 8.5.15. Enable encrypted data transmission according to PCI DSS Requirement 4.1. Enable account lockout after a certain number of failed login attempts according to PCI DSS Requirement 8.5.13. Configure the system so a remote user must establish a Virtual Private Network (VPN) connection via a firewall before access is allowed. Enable the

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						logging function. Restrict access to customer passwords to authorized reseller/integrator personnel.
18		Remote Access Service Detected	0.00	Low	Pass	**Policy Violation** **Port:** tcp/2020 One or more remote access services were detected on the remote host. As defined by the PCI ASV Program Guide: "remote access software includes, but is not limited to: VPN (IPSec, PPTP, SSL), pcAnywhere, VNC, Microsoft Terminal Server, remote web-based administration, ssh, Telnet." **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** ssh **Remediation:** Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix C or disabled/ removed. Please consult your ASV if you have questions about this Special Note.
19		SSHv2 Recon	5.00	Info	Pass	**Port:** tcp/2020 Trustkeeper was able to enumerate encryption ciphers available on an SSHv2 server. This is expected functionality of an SSH server and only represents an informational finding. **CVSSv2:** AV:N/AC:L/Au:N/C:P/I:N/A:N

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Service: ssh **Evidence:** SSHv2 Key Exchange Algorithms: diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1 SSHv2 Server Host Key Exchange Algorithms: ssh-rsa,ssh-dss SSHv2 Encryption Algorithms Client to Server: aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc, blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se SSHv2 Encryption Algorithms Server to Client: aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc, blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se SSHv2 MAC Algorithms Client to Server: hmac-md5,hmac-sha1, hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96, hmac-md5-96 SSHv2 MAC Algorithms Server to Client: hmac-md5,hmac-sha1, hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96, hmac-md5-96 SSHv2 Compression Algorithms Client to Server: none, zlib@openssh.com SSHv2 Compression Algorithms Server to Client: none, zlib@openssh.com SSHv2 Languages Client to Server: SSHv2 Languages Server to Client: **Remediation:** No remediation in necessary for this finding.

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
20		TCP Timestamp Options Enabled	0.00	Info	Pass	**Port:** tcp/21 The remote service supports TCP Timestamps, which are detailed in RFC1323. This information can potentially be used to discover the uptime of the remote system. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** ftp **Reference:** http://www.ietf.org/rfc/rfc1323.txt **Evidence:** Timestamp: 1580509239 **Remediation:** If you are concerned about the exposure of uptime of your systems, disable support for TCP Timestamps, if possible. This would be vendor specific.
21		Enumerated Applications	0.00	Info	Pass	**Port:** tcp/21 The following applications have been enumerated on this device. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** ftp **Evidence:** CPE: proftpd:proftpd Version: 1.3.4a

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: No remediation is required.
22		TCP Timestamp Options Enabled	0.00	Info	Pass	**Port:** tcp/25 The remote service supports TCP Timestamps, which are detailed in RFC1323. This information can potentially be used to discover the uptime of the remote system. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** smtp **Reference:** http://www.ietf.org/rfc/rfc1323.txt **Evidence:** Timestamp: 1580509214 **Remediation:** If you are concerned about the exposure of uptime of your systems, disable support for TCP Timestamps, if possible. This would be vendor specific.
23		SMTP Service Supports the STARTTLS Command	0.00	Info	Pass	**Port:** tcp/25 The SMTP service running on this host supports encryption using the STARTTLS command. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Service: smtp **Evidence:** Message: 220 ready for tls
24		OV/DV Certificate Detected	0.00	Info	Pass	**Port:** tcp/25 This SSL service appears to be using an SSL certificate that has been validated at either the organizational (OV) or domain (DV) levels. Modern web browsers recognize certificates that have been issued using a higher level of validation. Such certificates are known as Extended Validation, or "EV" certificates. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** smtp **Evidence:** Subject: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Issuer: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Certificate Chain Depth: 0 **Remediation:** Consider contacting your Certificate Authority (CA) about the availability of Extended Validation certificates. Since the number of CA's that are authorized to issue EV certificates increases regularly, it is possible that this finding may not be accurate. If you believe that you are already using an EV certificate, please

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						submit an appeal via the TrustKeeper user interface.
25		SSL Certificate Common Name Does Not Validate	0.00	Info	Pass	**Port:** tcp/25 This SSL certificate has a common name (CN) that does not appear to match the identity of the server. Modern browsers may present a warning to users who attempt to browse this service as it is currently configured. Note that in some networks in which load balancers are used, it may not be possible for the scanner to perform this test correctly. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** smtp **Evidence:** Subject: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Issuer: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Certificate Chain Depth: 0 Hostnames provided to scanner: www.mountaindropoffs.com, 78.109.167.20 Subject CN: plesk **Remediation:** Check your certificate to ensure it is installed on the correct service. Verify that you have added the domain name or fully qualified virtual host name of the system to your Network Questionnaire. Additionally, check your DNS servers to ensure

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						that the domain name is properly mapped to the correct IP address.
26		SSL Certificate is Self-Signed	0.00	Info	Pass	**Port:** tcp/25 This SSL certificate appears to be issued by a private Certificate Authority (CA). Users will likely receive a security warning if their client software (e.g., web browser) does not trust the issuer of the certificate. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** smtp **Evidence:** Subject: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Issuer: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Certificate Chain Depth: 0 **Remediation:** If this certificate is associated with a service accessible to the general public, you may want to consider acquiring a certificate from a well-known CA.
27		SSL Certificate is Not Trusted	0.00	Info	Pass	**Port:** tcp/25 It was not possible to validate the SSL certificate, and thus it could

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						not be trusted. Users may receive a security warning when using this service. This occurs because either the certificate or a certificate in its chain has issues that prevent validation. Some examples of these issues are, but not limited to, a certificate having expired, the hostname does not have match the name on the certificate, or the certificate is not signed by a well-known Certificate Authority (CA). **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** smtp **Evidence:** Subject: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Issuer: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Certificate Chain Depth: 0 Reason: The hostname on the certificate does not match any of the hostnames provided to the scanner. Reason: The leaf certificate is self-signed but is not trusted. **Remediation:** If this certificate is associated with a service accessible to the general public, you may want to consider acquiring a certificate from a well-known CA, and that it is not expired.
28		SSL Certificate Expired	0.00	Info	Pass	**Port:** tcp/25 This SSL certificate has expired. Users may receive a security

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						warning when they connect to this service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** smtp **Evidence:** Subject: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Issuer: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Certificate Chain Depth: 0 Expiration Date: 2013-02-01 13:06:25 UTC Scan Date: 2013-11-09 02:26:22 -0600 **Remediation:** Contact your Certificate Authority (CA) to have a new certificate issued.
29		SSL Ephemeral Diffie-Hellman Ciphers Supported	0.00	Info	Pass	**Port:** tcp/25 Ephemeral Diffie-Hellman ciphers can put undue processing burden on the server and could result in decreased performance. While the temporal key generation creates secure connections, servers with fewer resources may opt to disable ephemeral ciphers for the efficiency benefits. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** smtp

Vulnerability Scan Report: Vulnerability Details

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Reference: http://www.schneier.com/paper-ssl.pdf **Evidence:** Cipher Suite: SSLv3 : DHE-RSA-AES256-SHA Cipher Suite: SSLv3 : DHE-RSA-AES128-SHA Cipher Suite: SSLv3 : EDH-RSA-DES-CBC3-SHA Cipher Suite: SSLv3 : EDH-RSA-DES-CBC-SHA Cipher Suite: SSLv3 : EXP-EDH-RSA-DES-CBC-SHA Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : EDH-RSA-DES-CBC3-SHA Cipher Suite: TLSv1 : EDH-RSA-DES-CBC-SHA Cipher Suite: TLSv1 : EXP-EDH-RSA-DES-CBC-SHA **Remediation:** To disable ephemeral Diffie-Hellman ciphers in Apache, add '!kEDH' without quotes to your SSLCipherSuite directive in your Apache configuration files. Refer to the following Microsoft Knowledge Base article for instructions on how to disable certain cryptographic algorithms in Internet Information Server (IIS): http://support.microsoft.com/kb/245030. **Patches:** http://support.microsoft.com/kb/245030 http://httpd.apache.org/docs/2.2/ssl/

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
30		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	**Port:** tcp/25 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:** smtp **Reference:** http://www.openssl.org/docs/apps/ciphers.html **Evidence:** Cipher Suite: SSLv2 : DES-CBC3-MD5 Cipher Suite: SSLv2 : DES-CBC-MD5 Cipher Suite: SSLv2 : EXP-RC2-CBC-MD5 Cipher Suite: SSLv2 : RC2-CBC-MD5 Cipher Suite: SSLv2 : EXP-RC4-MD5 Cipher Suite: SSLv2 : RC4-MD5

Vulnerability Scan Report: Vulnerability Details

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: SSLv3 : DHE-RSA-AES256-SHA Cipher Suite: SSLv3 : AES256-SHA Cipher Suite: SSLv3 : DHE-RSA-AES128-SHA Cipher Suite: SSLv3 : AES128-SHA Cipher Suite: SSLv3 : EDH-RSA-DES-CBC3-SHA Cipher Suite: SSLv3 : EDH-RSA-DES-CBC-SHA Cipher Suite: SSLv3 : EXP-EDH-RSA-DES-CBC-SHA Cipher Suite: SSLv3 : DES-CBC3-SHA Cipher Suite: SSLv3 : DES-CBC-SHA Cipher Suite: SSLv3 : EXP-DES-CBC-SHA Cipher Suite: SSLv3 : EXP-RC2-CBC-MD5 Cipher Suite: SSLv3 : RC4-SHA Cipher Suite: SSLv3 : RC4-MD5 Cipher Suite: SSLv3 : EXP-RC4-MD5 Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : EDH-RSA-DES-CBC3-SHA Cipher Suite: TLSv1 : EDH-RSA-DES-CBC-SHA Cipher Suite: TLSv1 : EXP-EDH-RSA-DES-CBC-SHA Cipher Suite: TLSv1 : DES-CBC3-SHA Cipher Suite: TLSv1 : DES-CBC-SHA Cipher Suite: TLSv1 : EXP-DES-CBC-SHA Cipher Suite: TLSv1 : EXP-RC2-CBC-MD5 Cipher Suite: TLSv1 : RC4-SHA Cipher Suite: TLSv1 : RC4-MD5 Cipher Suite: TLSv1 : EXP-RC4-MD5 **Remediation:**

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						No remediation is necessary.
31	CVE-2011-3389	SSL Block-based Ciphers Supported	0.00	Info	Pass	**Port:** tcp/25 This server may be able to be configured to mitigate a vulnerability present in some web browsers. An attack, commonly known as "Browser Exploit Against SSL/TLS" ("BEAST"), takes advantage of this vulnerability in how the browser sets up SSL/TLS connections (e.g. for HTTPS), and may allow the attacker to decrypt the browser's SSL/TLS connection and gain access to sensitive information. The vulnerability is present on the browser, but steps may be taken on web servers to mitigate it. As the attack exploits block-based ciphers, SSL may be configured on web servers to disable block ciphers or to prefer stream-based ciphers (such as RC4) over block-based ones. Alternatively, the web server may be configured to allow only TLS versions 1.1 and 1.2, which are not vulnerable; however, support for these newer TLS versions is not as widespread, and disabling previous versions may prevent some users from connecting to the server. **CVE:** CVE-2011-3389 **NVD:** CVE-2011-3389 **Bugtraq:** 49778 **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** smtp **Reference:** https://bugzilla.mozilla.org/show_bug.cgi?id=665814 http://httpd.apache.org/docs/trunk/mod/mod_ssl.

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						html#sslciphersuite http://technet.microsoft.com/en-us/security/bulletin/ms12-006 http://support.microsoft.com/kb/2643584 http://technet.microsoft.com/en-us/security/advisory/2588513 **Evidence:** Cipher Suite: SSLv2 : DES-CBC3-MD5 Cipher Suite: SSLv2 : DES-CBC-MD5 Cipher Suite: SSLv2 : EXP-RC2-CBC-MD5 Cipher Suite: SSLv2 : RC2-CBC-MD5 Cipher Suite: SSLv3 : DHE-RSA-AES256-SHA Cipher Suite: SSLv3 : AES256-SHA Cipher Suite: SSLv3 : DHE-RSA-AES128-SHA Cipher Suite: SSLv3 : AES128-SHA Cipher Suite: SSLv3 : EDH-RSA-DES-CBC3-SHA Cipher Suite: SSLv3 : EDH-RSA-DES-CBC-SHA Cipher Suite: SSLv3 : EXP-EDH-RSA-DES-CBC-SHA Cipher Suite: SSLv3 : DES-CBC3-SHA Cipher Suite: SSLv3 : DES-CBC-SHA Cipher Suite: SSLv3 : EXP-DES-CBC-SHA Cipher Suite: SSLv3 : EXP-RC2-CBC-MD5 Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : EDH-RSA-DES-CBC3-SHA Cipher Suite: TLSv1 : EDH-RSA-DES-CBC-SHA Cipher Suite: TLSv1 : EXP-EDH-RSA-DES-CBC-SHA Cipher Suite: TLSv1 : DES-CBC3-SHA Cipher Suite: TLSv1 : DES-CBC-SHA

Vulnerability Scan Report: Vulnerability Details

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1 : EXP-DES-CBC-SHA Cipher Suite: TLSv1 : EXP-RC2-CBC-MD5
32	CVE-2013-2566	SSL RC4-based Ciphers Supported	0.00	Info	Pass	**Port:** tcp/25 This server may be able to be configured to mitigate a vulnerability present in some web browsers. An attack is possible when using RC4-based ciphers that takes advantage of single-byte biases within the RC4 algorithm, that could make it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of cipher text in a larger number of sessions (i. e. millions of sessions) that use the same plain text. The vulnerability is present on the browser, but steps may be taken on web servers to mitigate it. As the attack exploits RC4-based ciphers, SSL may be configured on web servers to disable RC4 ciphers or to prefer ciphers over RC4-based ones. Alternatively, the web server may be configured to allow only TLS versions 1.1 and 1.2, which are not vulnerable; however, support for these newer TLS versions is not as widespread, and disabling previous versions may prevent some users from connecting to the server. **CVE:** CVE-2013-2566 **NVD:** CVE-2013-2566 **CVSSv2:** AV:N/AC:H/Au:N/C:P/I:N/A:N **Service:** smtp **Evidence:** Cipher Suite: SSLv2 : EXP-RC4-MD5 Cipher Suite: SSLv2 : RC4-MD5

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: SSLv3 : RC4-SHA Cipher Suite: SSLv3 : RC4-MD5 Cipher Suite: SSLv3 : EXP-RC4-MD5 Cipher Suite: TLSv1 : RC4-SHA Cipher Suite: TLSv1 : RC4-MD5 Cipher Suite: TLSv1 : EXP-RC4-MD5
33		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 **Evidence:** CPE: apache:http_server Version: unknown **Remediation:** No remediation is required.
34		No X-FRAME-OPTIONS Header	0.00	Info	Pass	**Port:** tcp/80 This host does not appear to utilize the benefits that the X-FRAME-OPTIONS HTTP header element offers. This header may be implemented to prevent pages on this system from being used in part of a click-jacking scenario. The X-FRAME-OPTIONS header specifies what systems (if any) are allowed to refer to pages on this system (when the page is to appear within a HTML frame type of object).

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Reference:** https://www.owasp.org/index.php/Clickjacking#X-FRAME-OPTIONS **Remediation:** Consider utilizing the X-FRAME-OPTIONS header option to prevent click-jacking type of attacks.
35		Operating System Potentially Determined via Apache Requests	0.00	Info	Pass	**Port:** tcp/80 It was possible to potentially identify the remote operating system using various requests to the Apache service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Reference:** http://packetstormsecurity.org/files/view/71358/appOSfingerprint.txt **Evidence:** Potential Operating System: Unix/Linux **Remediation:** There is no solution at this time.

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
36		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 **Evidence:** URL: http://www.mountaindropoffs.com:80/cgi-bin/ HTTP Response Code: 403 URL: http://www.mountaindropoffs.com:80/error/ HTTP Response Code: 403 URL: http://www.mountaindropoffs.com:80/icons/ HTTP Response Code: 200 URL: http://www.mountaindropoffs.com:80/usage/ HTTP Response Code: 403 **Remediation:** Review these directories and verify that there is no unintentional content made available to remote users.
37		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

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Service: http **Evidence:** URL: http://www.mountaindropoffs.com/error/ Methods: GET, HEAD, POST, OPTIONS URL: http://www.mountaindropoffs.com/icons/ Methods: GET, HEAD, POST, OPTIONS **Remediation:** Review your web server configuration and ensure that only those HTTP methods required for your business operations are enabled.
38		OV/DV Certificate Detected	0.00	Info	Pass	**Port:** tcp/110 This SSL service appears to be using an SSL certificate that has been validated at either the organizational (OV) or domain (DV) levels. Modern web browsers recognize certificates that have been issued using a higher level of validation. Such certificates are known as Extended Validation, or "EV" certificates. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** pop3 **Evidence:** Subject: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Issuer: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Certificate Chain Depth: 0

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: Consider contacting your Certificate Authority (CA) about the availability of Extended Validation certificates. Since the number of CA's that are authorized to issue EV certificates increases regularly, it is possible that this finding may not be accurate. If you believe that you are already using an EV certificate, please submit an appeal via the TrustKeeper user interface.
39		SSL Certificate Common Name Does Not Validate	0.00	Info	Pass	**Port:** tcp/110 This SSL certificate has a common name (CN) that does not appear to match the identity of the server. Modern browsers may present a warning to users who attempt to browse this service as it is currently configured. Note that in some networks in which load balancers are used, it may not be possible for the scanner to perform this test correctly. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** pop3 **Evidence:** Subject: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Issuer: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Certificate Chain Depth: 0 Hostnames provided to scanner: www.mountaindropoffs.com, 78.109.167.20

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Subject CN: plesk **Remediation:** Check your certificate to ensure it is installed on the correct service. Verify that you have added the domain name or fully qualified virtual host name of the system to your Network Questionnaire. Additionally, check your DNS servers to ensure that the domain name is properly mapped to the correct IP address.
40		SSL Certificate is Self-Signed	0.00	Info	Pass	**Port:** tcp/110 This SSL certificate appears to be issued by a private Certificate Authority (CA). Users will likely receive a security warning if their client software (e.g., web browser) does not trust the issuer of the certificate. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** pop3 **Evidence:** Subject: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Issuer: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Certificate Chain Depth: 0 **Remediation:** If this certificate is associated with a service accessible to the

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						general public, you may want to consider acquiring a certificate from a well-known CA.
41		SSL Certificate is Not Trusted	0.00	Info	Pass	**Port:** tcp/110 It was not possible to validate the SSL certificate, and thus it could not be trusted. Users may receive a security warning when using this service. This occurs because either the certificate or a certificate in its chain has issues that prevent validation. Some examples of these issues are, but not limited to, a certificate having expired, the hostname does not have match the name on the certificate, or the certificate is not signed by a well-known Certificate Authority (CA). **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** pop3 **Evidence:** Subject: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Issuer: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Certificate Chain Depth: 0 Reason: The hostname on the certificate does not match any of the hostnames provided to the scanner. Reason: The leaf certificate is self-signed but is not trusted. **Remediation:** If this certificate is associated with a service accessible to the

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						general public, you may want to consider acquiring a certificate from a well-known CA, and that it is not expired.
42		SSL Certificate Expired	0.00	Info	Pass	**Port:** tcp/110 This SSL certificate has expired. Users may receive a security warning when they connect to this service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** pop3 **Evidence:** Subject: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Issuer: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Certificate Chain Depth: 0 Expiration Date: 2013-02-01 13:06:25 UTC Scan Date: 2013-11-09 02:26:24 -0600 **Remediation:** Contact your Certificate Authority (CA) to have a new certificate issued.
43		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	**Port:** tcp/110 The finding reports the SSL cipher suites for each SSL/TLS service version provided by the remote service. This finding does not

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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:** pop3 **Reference:** http://www.openssl.org/docs/apps/ciphers.html **Evidence:** Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : DES-CBC3-SHA Cipher Suite: TLSv1 : RC4-SHA Cipher Suite: TLSv1 : RC4-MD5 **Remediation:** No remediation is necessary.

Vulnerability Scan Report: Vulnerability Details

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
44	CVE-2011-3389	SSL Block-based Ciphers Supported	0.00	Info	Pass	**Port:** tcp/110 This server may be able to be configured to mitigate a vulnerability present in some web browsers. An attack, commonly known as "Browser Exploit Against SSL/TLS" ("BEAST"), takes advantage of this vulnerability in how the browser sets up SSL/TLS connections (e.g. for HTTPS), and may allow the attacker to decrypt the browser's SSL/TLS connection and gain access to sensitive information. The vulnerability is present on the browser, but steps may be taken on web servers to mitigate it. As the attack exploits block-based ciphers, SSL may be configured on web servers to disable block ciphers or to prefer stream-based ciphers (such as RC4) over block-based ones. Alternatively, the web server may be configured to allow only TLS versions 1.1 and 1.2, which are not vulnerable; however, support for these newer TLS versions is not as widespread, and disabling previous versions may prevent some users from connecting to the server. **CVE:** CVE-2011-3389 **NVD:** CVE-2011-3389 **Bugtraq:** 49778 **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** pop3 **Reference:** https://bugzilla.mozilla.org/show_bug.cgi?id=665814 http://httpd.apache.org/docs/trunk/mod/mod_ssl.html#sslciphersuite http://technet.microsoft.com/en-us/security/bulletin/ms12-006 http://support.microsoft.com/kb/2643584

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						http://technet.microsoft.com/en-us/security/advisory/2588513 **Evidence:** Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : DES-CBC3-SHA
45	CVE-2013-2566	SSL RC4-based Ciphers Supported	0.00	Info	Pass	**Port:** tcp/110 This server may be able to be configured to mitigate a vulnerability present in some web browsers. An attack is possible when using RC4-based ciphers that takes advantage of single-byte biases within the RC4 algorithm, that could make it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of cipher text in a larger number of sessions (i.e. millions of sessions) that use the same plain text. The vulnerability is present on the browser, but steps may be taken on web servers to mitigate it. As the attack exploits RC4-based ciphers, SSL may be configured on web servers to disable RC4 ciphers or to prefer ciphers over RC4-based ones. Alternatively, the web server may be configured to allow only TLS versions 1.1 and 1.2, which are not vulnerable; however, support for these newer TLS versions is not as widespread, and disabling previous versions may prevent some users from connecting to the server. **CVE:** CVE-2013-2566 **NVD:** CVE-2013-2566 **CVSSv2:** AV:N/AC:H/Au:N/C:P/I:N/A:N **Service:** pop3

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Evidence: Cipher Suite: TLSv1 : RC4-SHA Cipher Suite: TLSv1 : RC4-MD5
46		IMAP Service Supports the STARTTLS Command	0.00	Info	Pass	**Port:** tcp/143 The IMAP service running on this host supports encryption using the STARTTLS command. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** imap **Evidence:** Message: a001 OK Begin SSL/TLS negotiation now.
47		OV/DV Certificate Detected	0.00	Info	Pass	**Port:** tcp/143 This SSL service appears to be using an SSL certificate that has been validated at either the organizational (OV) or domain (DV) levels. Modern web browsers recognize certificates that have been issued using a higher level of validation. Such certificates are known as Extended Validation, or "EV" certificates. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** imap **Evidence:** Subject:

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						/C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Issuer: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Certificate Chain Depth: 0 **Remediation:** Consider contacting your Certificate Authority (CA) about the availability of Extended Validation certificates. Since the number of CA's that are authorized to issue EV certificates increases regularly, it is possible that this finding may not be accurate. If you believe that you are already using an EV certificate, please submit an appeal via the TrustKeeper user interface.
48		SSL Certificate Common Name Does Not Validate	0.00	Info	Pass	**Port:** tcp/143 This SSL certificate has a common name (CN) that does not appear to match the identity of the server. Modern browsers may present a warning to users who attempt to browse this service as it is currently configured. Note that in some networks in which load balancers are used, it may not be possible for the scanner to perform this test correctly. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** imap **Evidence:** Subject: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Issuer: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Certificate Chain Depth: 0 Hostnames provided to scanner: www.mountaindropoffs.com, 78.109.167.20 Subject CN: plesk **Remediation:** Check your certificate to ensure it is installed on the correct service. Verify that you have added the domain name or fully qualified virtual host name of the system to your Network Questionnaire. Additionally, check your DNS servers to ensure that the domain name is properly mapped to the correct IP address.
49		SSL Certificate is Self-Signed	0.00	Info	Pass	**Port:** tcp/143 This SSL certificate appears to be issued by a private Certificate Authority (CA). Users will likely receive a security warning if their client software (e.g., web browser) does not trust the issuer of the certificate. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** imap **Evidence:** Subject: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Issuer:

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						/C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Certificate Chain Depth: 0 **Remediation:** If this certificate is associated with a service accessible to the general public, you may want to consider acquiring a certificate from a well-known CA.
50		SSL Certificate is Not Trusted	0.00	Info	Pass	**Port:** tcp/143 It was not possible to validate the SSL certificate, and thus it could not be trusted. Users may receive a security warning when using this service. This occurs because either the certificate or a certificate in its chain has issues that prevent validation. Some examples of these issues are, but not limited to, a certificate having expired, the hostname does not have match the name on the certificate, or the certificate is not signed by a well-known Certificate Authority (CA). **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** imap **Evidence:** Subject: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Issuer: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Certificate Chain Depth: 0

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Reason: The hostname on the certificate does not match any of the hostnames provided to the scanner. Reason: The leaf certificate is self-signed but is not trusted. **Remediation:** If this certificate is associated with a service accessible to the general public, you may want to consider acquiring a certificate from a well-known CA, and that it is not expired.
51		SSL Certificate Expired	0.00	Info	Pass	**Port:** tcp/143 This SSL certificate has expired. Users may receive a security warning when they connect to this service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** imap **Evidence:** Subject: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Issuer: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Certificate Chain Depth: 0 Expiration Date: 2013-02-01 13:06:25 UTC Scan Date: 2013-11-09 02:26:24 -0600 **Remediation:** Contact your Certificate Authority (CA) to have a new certificate issued.

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
52		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	**Port:** tcp/143 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:** imap **Reference:** http://www.openssl.org/docs/apps/ciphers.html **Evidence:** Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : DES-CBC3-SHA Cipher Suite: TLSv1 : RC4-SHA Cipher Suite: TLSv1 : RC4-MD5

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: No remediation is necessary.
53	CVE-2011-3389	SSL Block-based Ciphers Supported	0.00	Info	Pass	**Port:** tcp/143 This server may be able to be configured to mitigate a vulnerability present in some web browsers. An attack, commonly known as "Browser Exploit Against SSL/TLS" ("BEAST"), takes advantage of this vulnerability in how the browser sets up SSL/TLS connections (e.g. for HTTPS), and may allow the attacker to decrypt the browser's SSL/TLS connection and gain access to sensitive information. The vulnerability is present on the browser, but steps may be taken on web servers to mitigate it. As the attack exploits block-based ciphers, SSL may be configured on web servers to disable block ciphers or to prefer stream-based ciphers (such as RC4) over block-based ones. Alternatively, the web server may be configured to allow only TLS versions 1.1 and 1.2, which are not vulnerable; however, support for these newer TLS versions is not as widespread, and disabling previous versions may prevent some users from connecting to the server. **CVE:** CVE-2011-3389 **NVD:** CVE-2011-3389 **Bugtraq:** 49778 **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** imap **Reference:**

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						https://bugzilla.mozilla.org/show_bug.cgi?id=665814 http://httpd.apache.org/docs/trunk/mod/mod_ssl.html#sslciphersuite http://technet.microsoft.com/en-us/security/bulletin/ms12-006 http://support.microsoft.com/kb/2643584 http://technet.microsoft.com/en-us/security/advisory/2588513 **Evidence:** Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : DES-CBC3-SHA
54	CVE-2013-2566	SSL RC4-based Ciphers Supported	0.00	Info	Pass	**Port:** tcp/143 This server may be able to be configured to mitigate a vulnerability present in some web browsers. An attack is possible when using RC4-based ciphers that takes advantage of single-byte biases within the RC4 algorithm, that could make it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of cipher text in a larger number of sessions (i.e. millions of sessions) that use the same plain text. The vulnerability is present on the browser, but steps may be taken on web servers to mitigate it. As the attack exploits RC4-based ciphers, SSL may be configured on web servers to disable RC4 ciphers or to prefer ciphers over RC4-based ones. Alternatively, the web server may be configured to allow only TLS versions 1.1 and 1.2, which are not vulnerable; however, support for these newer TLS versions is not as widespread, and disabling previous versions may prevent some users from connecting to the server.

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						CVE: CVE-2013-2566 **NVD:** CVE-2013-2566 **CVSSv2:** AV:N/AC:H/Au:N/C:P/I:N/A:N **Service:** imap **Evidence:** Cipher Suite: TLSv1 : RC4-SHA Cipher Suite: TLSv1 : RC4-MD5
55		OV/DV Certificate Detected	0.00	Info	Pass	**Port:** tcp/443 This SSL service appears to be using an SSL certificate that has been validated at either the organizational (OV) or domain (DV) levels. Modern web browsers recognize certificates that have been issued using a higher level of validation. Such certificates are known as Extended Validation, or "EV" certificates. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Evidence:** Subject: /OU=Domain Control Validated/OU=Hosted by UKFast.net Ltd/OU=COMODO SSL/CN=www.mountaindropoffs.com Issuer: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO SSL CA Certificate Chain Depth: 0 **Remediation:** Consider contacting your Certificate Authority (CA) about the

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						availability of Extended Validation certificates. Since the number of CA's that are authorized to issue EV certificates increases regularly, it is possible that this finding may not be accurate. If you believe that you are already using an EV certificate, please submit an appeal via the TrustKeeper user interface.
56		SSL Ephemeral Diffie-Hellman Ciphers Supported	0.00	Info	Pass	**Port:** tcp/443 Ephemeral Diffie-Hellman ciphers can put undue processing burden on the server and could result in decreased performance. While the temporal key generation creates secure connections, servers with fewer resources may opt to disable ephemeral ciphers for the efficiency benefits. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Reference:** http://www.schneier.com/paper-ssl.pdf **Evidence:** Cipher Suite: SSLv3 : DHE-RSA-AES256-SHA Cipher Suite: SSLv3 : DHE-RSA-AES128-SHA Cipher Suite: SSLv3 : EDH-RSA-DES-CBC3-SHA Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : EDH-RSA-DES-CBC3-SHA **Remediation:** To disable ephemeral Diffie-Hellman ciphers in Apache, add '!

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						kEDH' without quotes to your SSLCipherSuite directive in your Apache configuration files. Refer to the following Microsoft Knowledge Base article for instructions on how to disable certain cryptographic algorithms in Internet Information Server (IIS): http://support.microsoft.com/kb/245030. **Patches:** http://support.microsoft.com/kb/245030 http://httpd.apache.org/docs/2.2/ssl/
57		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

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Service: http **Reference:** http://www.openssl.org/docs/apps/ciphers.html **Evidence:** Cipher Suite: SSLv3 : DHE-RSA-AES256-SHA Cipher Suite: SSLv3 : AES256-SHA Cipher Suite: SSLv3 : DHE-RSA-AES128-SHA Cipher Suite: SSLv3 : AES128-SHA Cipher Suite: SSLv3 : EDH-RSA-DES-CBC3-SHA Cipher Suite: SSLv3 : DES-CBC3-SHA Cipher Suite: SSLv3 : RC4-SHA Cipher Suite: SSLv3 : RC4-MD5 Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : EDH-RSA-DES-CBC3-SHA Cipher Suite: TLSv1 : DES-CBC3-SHA Cipher Suite: TLSv1 : RC4-SHA Cipher Suite: TLSv1 : RC4-MD5 **Remediation:** No remediation is necessary.
58	CVE-2011-3389	SSL Block-based Ciphers Supported	0.00	Info	Pass	**Port:** tcp/443 This server may be able to be configured to mitigate a vulnerability present in some web browsers. An attack, commonly

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						known as "Browser Exploit Against SSL/TLS" ("BEAST"), takes advantage of this vulnerability in how the browser sets up SSL/TLS connections (e.g. for HTTPS), and may allow the attacker to decrypt the browser's SSL/TLS connection and gain access to sensitive information. The vulnerability is present on the browser, but steps may be taken on web servers to mitigate it. As the attack exploits block-based ciphers, SSL may be configured on web servers to disable block ciphers or to prefer stream-based ciphers (such as RC4) over block-based ones. Alternatively, the web server may be configured to allow only TLS versions 1.1 and 1.2, which are not vulnerable; however, support for these newer TLS versions is not as widespread, and disabling previous versions may prevent some users from connecting to the server. **CVE:** CVE-2011-3389 **NVD:** CVE-2011-3389 **Bugtraq:** 49778 **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Reference:** https://bugzilla.mozilla.org/show_bug.cgi?id=665814 http://httpd.apache.org/docs/trunk/mod/mod_ssl.html#sslciphersuite http://technet.microsoft.com/en-us/security/bulletin/ms12-006 http://support.microsoft.com/kb/2643584 http://technet.microsoft.com/en-us/security/advisory/2588513 **Evidence:**

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: SSLv3 : DHE-RSA-AES256-SHA Cipher Suite: SSLv3 : AES256-SHA Cipher Suite: SSLv3 : DHE-RSA-AES128-SHA Cipher Suite: SSLv3 : AES128-SHA Cipher Suite: SSLv3 : EDH-RSA-DES-CBC3-SHA Cipher Suite: SSLv3 : DES-CBC3-SHA Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : EDH-RSA-DES-CBC3-SHA Cipher Suite: TLSv1 : DES-CBC3-SHA
59	CVE-2013-2566	SSL RC4-based Ciphers Supported	0.00	Info	Pass	**Port:** tcp/443 This server may be able to be configured to mitigate a vulnerability present in some web browsers. An attack is possible when using RC4-based ciphers that takes advantage of single-byte biases within the RC4 algorithm, that could make it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of cipher text in a larger number of sessions (i.e. millions of sessions) that use the same plain text. The vulnerability is present on the browser, but steps may be taken on web servers to mitigate it. As the attack exploits RC4-based ciphers, SSL may be configured on web servers to disable RC4 ciphers or to prefer ciphers over RC4-based ones. Alternatively, the web server may be configured to allow only TLS versions 1.1 and 1.2, which are not vulnerable; however, support for these newer TLS versions is not as widespread, and disabling previous versions may prevent some users from connecting to the

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						server. **CVE:** CVE-2013-2566 **NVD:** CVE-2013-2566 **CVSSv2:** AV:N/AC:H/Au:N/C:P/I:N/A:N **Service:** http **Evidence:** Cipher Suite: SSLv3 : RC4-SHA Cipher Suite: SSLv3 : RC4-MD5 Cipher Suite: TLSv1 : RC4-SHA Cipher Suite: TLSv1 : RC4-MD5
60		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 **Evidence:** CPE: apache:http_server Version: unknown **Remediation:** No remediation is required.
61		No X-FRAME-OPTIONS Header	0.00	Info	Pass	**Port:** tcp/443

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						This host does not appear to utilize the benefits that the X-FRAME-OPTIONS HTTP header element offers. This header may be implemented to prevent pages on this system from being used in part of a click-jacking scenario. The X-FRAME-OPTIONS header specifies what systems (if any) are allowed to refer to pages on this system (when the page is to appear within a HTML frame type of object). **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Reference:** https://www.owasp.org/index.php/Clickjacking#X-FRAME-OPTIONS **Remediation:** Consider utilizing the X-FRAME-OPTIONS header option to prevent click-jacking type of attacks.
62		Operating System Potentially Determined via Apache Requests	0.00	Info	Pass	**Port:** tcp/443 It was possible to potentially identify the remote operating system using various requests to the Apache service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Reference:** http://packetstormsecurity.org/files/view/71358/appOSfingerprint.txt **Evidence:**

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Potential Operating System: Unix/Linux **Remediation:** There is no solution at this time.
63		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 **Evidence:** URL: https://www.mountaindropoffs.com:443/cgi-bin/ HTTP Response Code: 403 URL: https://www.mountaindropoffs.com:443/error/ HTTP Response Code: 403 URL: https://www.mountaindropoffs.com:443/fr/ HTTP Response Code: 200 URL: https://www.mountaindropoffs.com:443/icons/ HTTP Response Code: 200 URL: https://www.mountaindropoffs.com:443/usage/ HTTP Response Code: 403 **Remediation:** Review these directories and verify that there is no unintentional content made available to remote users.

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
64		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/443 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: https://www.mountaindropoffs.com/en/login/ **Remediation:**

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
65		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/443 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Evidence: URL: https://www.mountaindropoffs.com/en/contact-details **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
66		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/443 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Reference: http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: https://www.mountaindropoffs.com/en/frequently-asked-questions **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
67		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/443 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: https://www.mountaindropoffs.com/en/site_help **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
68		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/443 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: https://www.mountaindropoffs.com/en/site_help/unsubscribe **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
69		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/443

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: https://www.mountaindropoffs.com/en/terms-and-conditions **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						links will provide information on the proper ways for indicating the character set encoding.
70		Web Application Potentially Sensitive CGI Parameter Detection	0.00	Info	Pass	**Port:** tcp/443 According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Evidence:** Location: https://www.mountaindropoffs.com/en/login/ Form Name: (no name) Fields: username (Potential horizontal privilege escalation - try another user ID), password (Possibly a clear or hashed password, vulnerable to sniffing or dictionary attack) **Remediation:** The parameters for this server should be examined to determine what type of data is controlled and if it poses a security risk.
71		Web Application Potentially Sensitive CGI Parameter Detection	0.00	Info	Pass	**Port:** tcp/443 According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						may disclose sensitive data or be prone to tampering that could result in privilege escalation. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Evidence:** Location: https://www.mountaindropoffs.com/booking/booking.php?lang=en/ Form Name: booking Fields: pass (Possibly a clear or hashed password, vulnerable to sniffing or dictionary attack), pass2 (Possibly a clear or hashed password, vulnerable to sniffing or dictionary attack), username (Potential horizontal privilege escalation - try another user ID) **Remediation:** The parameters for this server should be examined to determine what type of data is controlled and if it poses a security risk.
72		Web Application Potentially Sensitive CGI Parameter Detection	0.00	Info	Pass	**Port:** tcp/443 According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Evidence:**

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Location: https://www.mountaindropoffs.com/fr/login/ Form Name: (no name) Fields: username (Potential horizontal privilege escalation - try another user ID), password (Possibly a clear or hashed password, vulnerable to sniffing or dictionary attack) **Remediation:** The parameters for this server should be examined to determine what type of data is controlled and if it poses a security risk.
73		Web Application Potentially Sensitive CGI Parameter Detection	0.00	Info	Pass	**Port:** tcp/443 According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Evidence:** Location: https://www.mountaindropoffs.com/booking/booking.php?lang=fr/ Form Name: booking Fields: pass (Possibly a clear or hashed password, vulnerable to sniffing or dictionary attack), pass2 (Possibly a clear or hashed password, vulnerable to sniffing or dictionary attack), username (Potential horizontal privilege escalation - try another user ID) **Remediation:**

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						The parameters for this server should be examined to determine what type of data is controlled and if it poses a security risk.
74		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 **Evidence:** URL: https://www.mountaindropoffs.com/error/ Methods: GET, HEAD, POST, OPTIONS URL: https://www.mountaindropoffs.com/icons/ Methods: GET, HEAD, POST, OPTIONS URL: https://www.mountaindropoffs.com/Scripts/ Methods: GET, HEAD, POST, OPTIONS **Remediation:** Review your web server configuration and ensure that only those HTTP methods required for your business operations are enabled.
75		Non-HttpOnly Session Cookies Identified	0.00	Info	Pass	**Port:** tcp/443 The website software running on this server appears to be setting session cookies without the HttpOnly flag set. This means the session identifier information in these cookies is more susceptable

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						to attacks such as XSS which may allow attackers to read this cookie's data. **CVSSv2:** AV:N/AC:H/Au:N/C:P/I:P/A:N **Service:** http **Reference:** https://www.owasp.org/index.php/HttpOnly http://msdn.microsoft.com/en-us/library/system.web.httpcookie.httponly.aspx **Evidence:** URL: https://www.mountaindropoffs.com/fr/ Cookie Name: PHPSESSID Cookie Value: ecqs51otp2hmkfu5hjgm9rn2l0 Cookie HttpOnly Flag: false **Remediation:** Contact the vendor of this web application and request the HttpOnly flag be set on session cookies.
76		Enumerated Applications	0.00	Info	Pass	**Port:** tcp/2020 The following applications have been enumerated on this device. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** ssh **Evidence:** CPE: openssh:openssh

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Version: 4.3 **Remediation:** No remediation is required.
77		OV/DV Certificate Detected	0.00	Info	Pass	**Port:** tcp/8443 This SSL service appears to be using an SSL certificate that has been validated at either the organizational (OV) or domain (DV) levels. Modern web browsers recognize certificates that have been issued using a higher level of validation. Such certificates are known as Extended Validation, or "EV" certificates. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Evidence:** Subject: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Issuer: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Certificate Chain Depth: 0 **Remediation:** Consider contacting your Certificate Authority (CA) about the availability of Extended Validation certificates. Since the number of CA's that are authorized to issue EV certificates increases regularly, it is possible that this finding may not be accurate. If you believe that you are already using an EV certificate, please

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						submit an appeal via the TrustKeeper user interface.
78		SSL Certificate Common Name Does Not Validate	0.00	Info	Pass	**Port:** tcp/8443 This SSL certificate has a common name (CN) that does not appear to match the identity of the server. Modern browsers may present a warning to users who attempt to browse this service as it is currently configured. Note that in some networks in which load balancers are used, it may not be possible for the scanner to perform this test correctly. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Evidence:** Subject: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Issuer: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Certificate Chain Depth: 0 Hostnames provided to scanner: www.mountaindropoffs.com, 78.109.167.20 Subject CN: plesk **Remediation:** Check your certificate to ensure it is installed on the correct service. Verify that you have added the domain name or fully qualified virtual host name of the system to your Network Questionnaire. Additionally, check your DNS servers to ensure

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						that the domain name is properly mapped to the correct IP address.
79		SSL Certificate is Self-Signed	0.00	Info	Pass	**Port:** tcp/8443 This SSL certificate appears to be issued by a private Certificate Authority (CA). Users will likely receive a security warning if their client software (e.g., web browser) does not trust the issuer of the certificate. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Evidence:** Subject: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Issuer: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Certificate Chain Depth: 0 **Remediation:** If this certificate is associated with a service accessible to the general public, you may want to consider acquiring a certificate from a well-known CA.
80		SSL Certificate is Not Trusted	0.00	Info	Pass	**Port:** tcp/8443 It was not possible to validate the SSL certificate, and thus it could

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						not be trusted. Users may receive a security warning when using this service. This occurs because either the certificate or a certificate in its chain has issues that prevent validation. Some examples of these issues are, but not limited to, a certificate having expired, the hostname does not have match the name on the certificate, or the certificate is not signed by a well-known Certificate Authority (CA). **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Evidence:** Subject: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Issuer: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Certificate Chain Depth: 0 Reason: The hostname on the certificate does not match any of the hostnames provided to the scanner. Reason: The leaf certificate is self-signed but is not trusted. **Remediation:** If this certificate is associated with a service accessible to the general public, you may want to consider acquiring a certificate from a well-known CA, and that it is not expired.
81		SSL Certificate Expired	0.00	Info	Pass	**Port:** tcp/8443 This SSL certificate has expired. Users may receive a security

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						warning when they connect to this service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Evidence:** Subject: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Issuer: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Certificate Chain Depth: 0 Expiration Date: 2013-02-01 13:06:25 UTC Scan Date: 2013-11-09 02:26:20 -0600 **Remediation:** Contact your Certificate Authority (CA) to have a new certificate issued.
82		SSL Ephemeral Diffie-Hellman Ciphers Supported	0.00	Info	Pass	**Port:** tcp/8443 Ephemeral Diffie-Hellman ciphers can put undue processing burden on the server and could result in decreased performance. While the temporal key generation creates secure connections, servers with fewer resources may opt to disable ephemeral ciphers for the efficiency benefits. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Reference: http://www.schneier.com/paper-ssl.pdf **Evidence:** Cipher Suite: SSLv3 : DHE-RSA-AES256-SHA Cipher Suite: SSLv3 : DHE-RSA-AES128-SHA Cipher Suite: SSLv3 : EDH-RSA-DES-CBC3-SHA Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : EDH-RSA-DES-CBC3-SHA **Remediation:** To disable ephemeral Diffie-Hellman ciphers in Apache, add '!kEDH' without quotes to your SSLCipherSuite directive in your Apache configuration files. Refer to the following Microsoft Knowledge Base article for instructions on how to disable certain cryptographic algorithms in Internet Information Server (IIS): http://support.microsoft.com/kb/245030. **Patches:** http://support.microsoft.com/kb/245030 http://httpd.apache.org/docs/2.2/ssl/
83		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	**Port:** tcp/8443 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

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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: SSLv3 : DHE-RSA-AES256-SHA Cipher Suite: SSLv3 : AES256-SHA Cipher Suite: SSLv3 : DHE-RSA-AES128-SHA Cipher Suite: SSLv3 : AES128-SHA Cipher Suite: SSLv3 : EDH-RSA-DES-CBC3-SHA Cipher Suite: SSLv3 : DES-CBC3-SHA Cipher Suite: SSLv3 : RC4-SHA Cipher Suite: SSLv3 : RC4-MD5 Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : EDH-RSA-DES-CBC3-SHA Cipher Suite: TLSv1 : DES-CBC3-SHA Cipher Suite: TLSv1 : RC4-SHA Cipher Suite: TLSv1 : RC4-MD5 **Remediation:** No remediation is necessary.
84	CVE-2011-3389	SSL Block-based Ciphers Supported	0.00	Info	Pass	**Port:** tcp/8443 This server may be able to be configured to mitigate a vulnerability present in some web browsers. An attack, commonly known as "Browser Exploit Against SSL/TLS" ("BEAST"), takes advantage of this vulnerability in how the browser sets up SSL/TLS connections (e.g. for HTTPS), and may allow the attacker to decrypt the browser's SSL/TLS connection and gain access to sensitive information. The vulnerability is present on the browser, but steps may be taken on web servers to mitigate it. As the attack exploits block-based ciphers, SSL may be configured on web servers to disable block ciphers or to prefer stream-based ciphers (such as RC4) over block-based ones. Alternatively, the web server may be configured to allow only TLS versions 1.1 and 1.2, which are not vulnerable; however, support for these newer TLS versions is not as widespread, and disabling previous versions may prevent some users from connecting to the server. **CVE:** CVE-2011-3389 **NVD:** CVE-2011-3389

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Bugtraq: 49778 **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Reference:** https://bugzilla.mozilla.org/show_bug.cgi?id=665814 http://httpd.apache.org/docs/trunk/mod/mod_ssl.html#sslciphersuite http://technet.microsoft.com/en-us/security/bulletin/ms12-006 http://support.microsoft.com/kb/2643584 http://technet.microsoft.com/en-us/security/advisory/2588513 **Evidence:** Cipher Suite: SSLv3 : DHE-RSA-AES256-SHA Cipher Suite: SSLv3 : AES256-SHA Cipher Suite: SSLv3 : DHE-RSA-AES128-SHA Cipher Suite: SSLv3 : AES128-SHA Cipher Suite: SSLv3 : EDH-RSA-DES-CBC3-SHA Cipher Suite: SSLv3 : DES-CBC3-SHA Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : EDH-RSA-DES-CBC3-SHA Cipher Suite: TLSv1 : DES-CBC3-SHA
85	CVE-2013-2566	SSL RC4-based Ciphers Supported	0.00	Info	Pass	**Port:** tcp/8443 This server may be able to be configured to mitigate a vulnerability present in some web browsers. An attack is possible

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						when using RC4-based ciphers that takes advantage of single-byte biases within the RC4 algorithm, that could make it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of cipher text in a larger number of sessions (i.e. millions of sessions) that use the same plain text. The vulnerability is present on the browser, but steps may be taken on web servers to mitigate it. As the attack exploits RC4-based ciphers, SSL may be configured on web servers to disable RC4 ciphers or to prefer ciphers over RC4-based ones. Alternatively, the web server may be configured to allow only TLS versions 1.1 and 1.2, which are not vulnerable; however, support for these newer TLS versions is not as widespread, and disabling previous versions may prevent some users from connecting to the server. **CVE:** CVE-2013-2566 **NVD:** CVE-2013-2566 **CVSSv2:** AV:N/AC:H/Au:N/C:P/I:N/A:N **Service:** http **Evidence:** Cipher Suite: SSLv3 : RC4-SHA Cipher Suite: SSLv3 : RC4-MD5 Cipher Suite: TLSv1 : RC4-SHA Cipher Suite: TLSv1 : RC4-MD5
86		No X-FRAME-OPTIONS Header	0.00	Info	Pass	**Port:** tcp/8443 This host does not appear to utilize the benefits that the X-FRAME-OPTIONS HTTP header element offers. This header may be

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						implemented to prevent pages on this system from being used in part of a click-jacking scenario. The X-FRAME-OPTIONS header specifies what systems (if any) are allowed to refer to pages on this system (when the page is to appear within a HTML frame type of object). **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Reference:** https://www.owasp.org/index.php/Clickjacking#X-FRAME-OPTIONS **Remediation:** Consider utilizing the X-FRAME-OPTIONS header option to prevent click-jacking type of attacks.
87		Enumerated Applications	0.00	Info	Pass	**Port:** tcp/8443 The following applications have been enumerated on this device. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Evidence:** CPE: parallels:parallels_plesk_panel URI: / Version: 11.0.9-110120608.16 **Remediation:** No remediation is required.

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
88		Discovered Web Directories	0.00	Info	Pass	**Port:** tcp/8443 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 **Evidence:** URL: https://www.mountaindropoffs.com:8443/admin/ HTTP Response Code: 200 **Remediation:** Review these directories and verify that there is no unintentional content made available to remote users.
89		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/8443 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: https://www.mountaindropoffs.com:8443/admin/ **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
90		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/8443 During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: https://www.mountaindropoffs.com:8443/index.php **Remediation:** It's important that all documents served by the HTTP server provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
91		HTTP Responses Missing	0.00	Info	Pass	**Port:** tcp/8443

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
		Character Encoding				During the crawl of the HTTP service, we detected HTML and/or XML documents that were missing any indication of their character set encoding. The server and the pages it serves are responsible for indicating the character set used to encode the documents. Typically, these are indicated within the "Content-type" HTTP header, a 'meta' HTTP-equiv HTML tag, or an XML document encoding header. Without these, some web browsers may attempt to guess the character set encoding of the document by making a guess based on whats available. The danger in this is when browsers guess the incorrect encoding, resulting in a misinterpretation of the document. In cases where a webpage will reflect user-supplied information, an attacker could provide a specially-crafted string that could trick a web browser into decoding the document as a specific character set. If this specially-crafted string were HTML code encoded in the character set, the attacker could perform a cross-site scripting attack. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: https://www.mountaindropoffs.com:8443/ **Remediation:** It's important that all documents served by the HTTP server

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						provide the correct character set for their encoding. The provided links will provide information on the proper ways for indicating the character set encoding.
92		Web Application Potentially Sensitive CGI Parameter Detection	0.00	Info	Pass	**Port:** tcp/8443 According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Evidence:** Location: https://www.mountaindropoffs.com:8443/login_up.php3 Form Name: (no name) Fields: passwd (Possibly a clear or hashed password, vulnerable to sniffing or dictionary attack) **Remediation:** The parameters for this server should be examined to determine what type of data is controlled and if it poses a security risk.
93		Web Application Potentially Sensitive CGI Parameter Detection	0.00	Info	Pass	**Port:** tcp/8443 According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Evidence:** Location: https://www.mountaindropoffs.com:8443/get_password.php Form Name: (no name) Fields: cmd (Possibly a command - try 'edit', 'view', 'delete', etc) **Remediation:** The parameters for this server should be examined to determine what type of data is controlled and if it poses a security risk.
94		Discovered HTTP Methods	0.00	Info	Pass	**Port:** tcp/8443 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 **Evidence:** URL: https://www.mountaindropoffs.com:8443/javascript/

78.109.167.20

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Methods: OPTIONS, GET, HEAD, POST URL: https://www.mountaindropoffs.com:8443/skins/ Methods: OPTIONS, GET, HEAD, POST **Remediation:** Review your web server configuration and ensure that only those HTTP methods required for your business operations are enabled.
95		Discovered Web Applications	0.00	Info	Pass	**Port:** tcp/8443 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 **Evidence:** Name: parallels:parallels_plesk_panel Version: 11.0.9-110120608.16 URL: https://www.mountaindropoffs.com:8443/ **Remediation:** No remediation is required.
96		POP3 Service Supports the STARTTLS Command		Info	Pass	**Port:** tcp/110 The POP3 service running on this host supports encryption using the STARTTLS command.

Vulnerability Scan Report: Vulnerability Details

78.109.167.20						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Service: pop3 **Evidence:** Message: +OK Begin SSL/TLS negotiation now.

Part 5a. Web Servers

It is important to pay special attention to the security of your Web servers. This section provides a convenient list of all of the Web servers found in the course of the network scan based on the locations you specified in your scan setup. Information profiled includes the server type (e.g., Microsoft IIS or Apache) and the title of the default Web page. Some tips for using this information are below.

- You should ensure that all Web servers listed in this section are authorized and intended to be running in your network since many systems will inadvertently be configured with some type of Web server when they are installed.
- In addition, many network devices (e.g., routers, switches and print servers) may have Web-based management interfaces of which you may not have been aware. Whenever possible, unused Web interfaces should be disabled or, at a minimum, password protected.
- Review the "Port" column and make sure that any sites that should be secure are using port 443 (HTTPS, or "Secure Web") to encrypt the web sessions.

Special Note: If you are using load balancers for your web sites to spread the web traffic across multiple servers, it is your responsibility to ensure that the configuration of the environment behind your load balancers is synchronized, or to ensure that the environment is scanned as part of the internal vulnerability scans required by PCI DSS.

#	System IP Address	Domain Name	Port	Server Type	Default Status and Title/Redirect
1	78.109.167.20	mailserv.mountaindropoffs.com	tcp / 80	apache:http_server	
2			tcp / 443		
3			tcp / 8443		

Part 5b. SSL Certificate Information

Several network services, most notably HTTPS ("Secure Web"), employ certificates which contain information about the service which can be used by connecting clients to authenticate the identity of the server. For Web servers, the certificate is intended to authenticate the domain name (e.g., www.yoursite.com) of a web site. For example, a home banking application should be run on a web server which provides a certificate to its clients' Web browsers proving that the web server they are connected to is actually the one they intended to use.
In order to provide users with confidence in the site they are visiting, the certificate should be issued by a well-known certificate authority instead of self-generated. In some cases, such as in a private network, self-generated certificates may be used; however, those users should have confidence in the internal issuing authority.
This table provides a summary of the certificates found in your network, including expiration date and issuer of each certificate.

#	Service	Common Name	Expires	Details
1	78.109.167.20 : 25 (smtp)	plesk	2/1/13 7:06 AM	Issued to: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Issued by: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Fingerprint:4E:D3:67:8D:C3:10:B2:61:E1:8D:D7:1E:78:56:B5:EF
2	78.109.167.20 : 110 (pop3)	plesk	2/1/13 7:06 AM	Issued to: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Issued by: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Fingerprint:4E:D3:67:8D:C3:10:B2:61:E1:8D:D7:1E:78:56:B5:EF
3	78.109.167.20 : 143 (imap)	plesk	2/1/13 7:06 AM	Issued to: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Issued by:

Vulnerability Scan Report: Vulnerability Details

#	Service	Common Name	Expires	Details
				/C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Fingerprint:4E:D3:67:8D:C3:10:B2:61:E1:8D:D7:1E:78:56:B5:EF
4	78.109.167.20 : 443 (http)	www.mountaindropoffs.com	7/24/14 6:59 PM	Issued to: /OU=Domain Control Validated/OU=Hosted by UKFast.net Ltd/OU=COMODO SSL/CN=www.mountaindropoffs.com Issued by: /C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=COMODO SSL CA Fingerprint:57:CD:67:A0:86:6A:93:A1:EC:2E:D8:44:AC:FC:A3:E4
5	78.109.167.20 : 8443 (http)	plesk	2/1/13 7:06 AM	Issued to: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Issued by: /C=US/ST=Virginia/L=Herndon/O=Parallels/OU=Plesk/CN=plesk/emailAddress=info@plesk.com Fingerprint:4E:D3:67:8D:C3:10:B2:61:E1:8D:D7:1E:78:56:B5:EF

Part 6. Disputed Vulnerabilities & Policy Violations

The following vulnerabilities and policy violations were successfully disputed by you and have been removed from the scoring of your report. These items no longer affect any compliance assessment that this report may support. All disputes listed here were approved based on information which you have provided and represented and warranted to be complete and accurate.

#	Severity	IP Address & Port	Expires	Detail
1	High	78.109.167.20:2020	2014-01-15 14:32:13	OpenSSH < 4.4 Multiple Vulnerabilities **Disputed By:** Trustwave Support **Disputed Date:** 2013-11-09 03:13:22 **Reference Id:** 783895 **Approved Date:** 2013-11-09 03:13:22 **User Name** / **Comment**: Trustwave Support / AUTO_CONFIRMED by false positive analysis
2	High	78.109.167.20:2020	2014-01-15 14:31:39	OpenSSH Privilege Separation Monitor Weakness **Disputed By:** Trustwave Support **Disputed Date:** 2013-11-09 03:13:22 **Reference Id:** 783896 **Approved Date:** 2013-11-09 03:13:22 **User Name** / **Comment**: Trustwave Support / AUTO_CONFIRMED by false positive analysis
3	High	78.109.167.20:2020	2014-01-06 13:47:45	OpenSSH X11 Cookie Local Authentication Bypass Vulnerability **Disputed By:** Trustwave Support **Disputed Date:** 2013-11-09 03:13:22 **Reference Id:** 783897 **Approved Date:** 2013-11-09 03:13:22 **User Name** / **Comment**: Trustwave Support / AUTO_CONFIRMED by false positive analysis

Vulnerability Scan Report: Vulnerability Details

#	Severity	IP Address & Port	Expires	Detail
4	Medium	78.109.167.20:25	2014-01-06 13:48:39	SSLv2 Supported **Disputed By:** Trustwave Support **Disputed Date:** 2013-11-09 03:13:22 **Reference Id:** 783894 **Approved Date:** 2013-11-09 03:13:22 **User Name** / **Comment** Trustwave Support / AUTO_CONFIRMED by false positive analysis

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:	