Trustwave®

Report Date: 2017-03-05

Vulnerability Scan Report: Attestation of Compliance

Scan Customer Information				Approved Scanning Vendor Information			
Company Name:	ANTIQUE ROSE AND HERB FARM			**Company Name:**	Trustwave Holdings, Inc.		
Contact:	TRACI ANDERSON	**Title:**		**Contact:**	Trustwave Support	**URL:**	www.trustwave.com
Telephone:	352-357-2643	**E-mail:**	INFO@ROSESANDHERBS.COM	**Telephone:**	1-800-363-1621	**E-mail:**	support@trustwave.com
Business Address:	34935 WEST HUFF ROAD			**Business Address:**	70 West Madison St., Ste 1050		
City:	EUSTIS	**State/Province:**	Florida	**City:**	Chicago	**State/Province:**	IL
ZIP/Postal Code:	32736	**Country:**	US	**ZIP/Postal Code:**	60602	**Country:**	US

Scan Status

Fail	Scan Compliance Status
2	Number of unique components scanned that are in scope
8	Number of identified failing vulnerabilities
0	Number of components scanned by TrustKeeper but confirmed by the customer not to be in scope
2016-12-07	Date Scan Completed
N/A	Scan Expiration Date (3 months from Date Scan Completed)

Scan Customer Attestation

ANTIQUE ROSE AND HERB FARM 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. ANTIQUE ROSE AND HERB FARM 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 ANTIQUE ROSE AND HERB FARMs 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 3702-01-11 (2016), 3702-01-10 (2015), 3702-01-09 (2014), 3702-01-08 (2013), 3702-01-07 (2012), 3702-01-06 (2011), 3702-01-05 (2010), according to internal processes that meet PCI DSS requirement 11.2 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.

Vulnerability Scan Report: Table of Contents

Attestation of Compliance **1**

Executive Summary **3**

Part 1. Scan Information 3

Part 2. Component Compliance Summary 3

Part 3a. Vulnerabilities Noted for Each IP Address 3

Part 3b. Special Notes by IP Address 7

Vulnerability Details **8**

Part 1. Scan Information 8

Part 2. Scan Inventory (Accessible Systems and Services) 8

Part 3a. Previous Scan Targets (Not Scanned) 11

Part 3b. Discovered Scan Targets (Not Scanned) 11

Part 3c. Load Balancers 12

Part 4. Vulnerability & Policy Violations 13

199.48.239.47 (www.rosesandherbs.com) 13

Part 5a. Web Servers 86

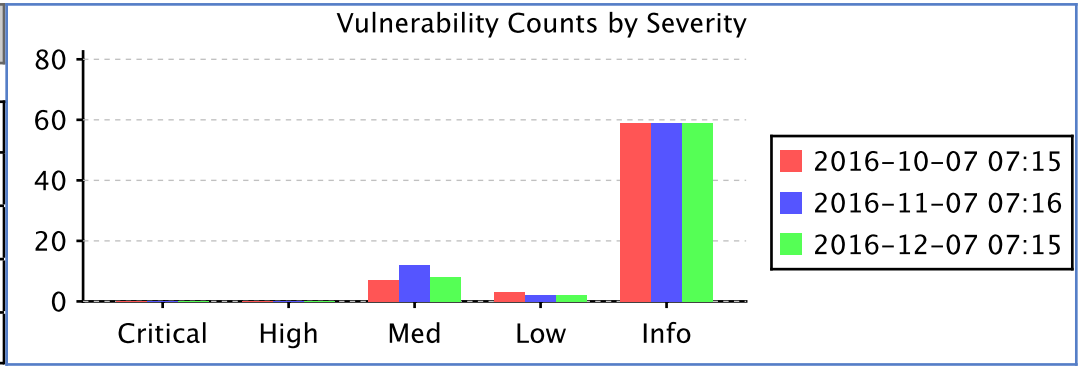
Part 5b. SSL Certificate Information 87

Part 6. Disputed Vulnerability & Policy Violations 89

Vulnerability Scan Report: Executive Summary

Part 1. Scan Information

Scan Customer Company	ANTIQUE ROSE AND HERB FARM
ASV Company	Trustwave Holdings, Inc.
Scan Compliance Status	Fail
Date Scan Completed	2016-12-07
Scan Expiration Date	N/A



Part 2. Component Compliance Summary

#	Compliance Status	Name	Type	IP Address	Source	Critical	High	Medium	Low	Info
1	Pass	71.49.118.68 (office)	Physical	71.49.118.68	IP Address	0	0	0	0	0
2	Fail	www.rosesandherbs.com	Web Site	199.48.239.47	Domain Name	0	0	8	2	59
					Total Findings	**0**	**0**	**8**	**2**	**59**
					Total PCI Vulnerabilities	**0**	**0**	**8**	**0**	**0**

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	199.48.239.47 (www.	Basic Authentication over HTTP	Medium	6.10	Fail	**Note to scan customer:** Unencrypted communication channels violate Requirement 4 of the PCI DSS and are considered an automatic failing condition. This

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
	rosesandherbs.com)					vulnerability is not recognized in the National Vulnerability Database.
2	199.48.239.47 (www.rosesandherbs.com)	Block cipher algorithms with block size of 64 bits (like DES and 3DES) birthday attack known as Sweet32, CVE-2016-2183	Medium	5.00	Fail	
3	199.48.239.47 (www.rosesandherbs.com)	TLSv1.0 Supported	Medium	5.00	Fail	**Note to scan customer:** TLS v1.0 violates PCI DSS and is considered an automatic failing condition. This vulnerability is not recognized in the National Vulnerability Database.
4	199.48.239.47 (www.rosesandherbs.com)	Web Application Transmits Login Credentials Without Encryption	Medium	4.60	Fail	
5	199.48.239.47 (www.rosesandherbs.com)	No X-FRAME-OPTIONS Header	Low	2.60	Pass	**Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database.
6	199.48.239.47 (www.rosesandherbs.com)	Discovered HTTP Methods	Info	0.00	Pass	
7	199.48.239.47 (www.rosesandherbs.com)	Discovered Web Directories	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
8	199.48.239.47 (www.rosesandherbs.com)	Enumerated Hostnames	Info	0.00	Pass	
9	199.48.239.47 (www.rosesandherbs.com)	Enumerated SSL/TLS Cipher Suites	Info	0.00	Pass	
10	199.48.239.47 (www.rosesandherbs.com)	FrontPage Detected	Info	0.00	Pass	
11	199.48.239.47 (www.rosesandherbs.com)	FTP Server Supports AUTH TLS (STARTTLS)	Info	0.00	Pass	
12	199.48.239.47 (www.rosesandherbs.com)	HTTP Responses Missing Character Encoding	Info	0.00	Pass	
13	199.48.239.47 (www.rosesandherbs.com)	Operating System Potentially Determined via Apache Requests	Info	0.00	Pass	
14	199.48.239.47 (www.rosesandherbs.com)	Protected Web Page	Info	0.00	Pass	
15	199.48.239.47	SMTP Service Supports the	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
	(www.rosesandherbs.com)	STARTTLS Command				
16	199.48.239.47 (www.rosesandherbs.com)	SSL Certificate Chain Not Trusted	Info	0.00	Pass	
17	199.48.239.47 (www.rosesandherbs.com)	SSL Certificate Common Name Does Not Validate	Info	0.00	Pass	
18	199.48.239.47 (www.rosesandherbs.com)	SSL Certificate is Not Trusted	Info	0.00	Pass	
19	199.48.239.47 (www.rosesandherbs.com)	SSL Perfect Forward Secrecy Supported	Info	0.00	Pass	
20	199.48.239.47 (www.rosesandherbs.com)	SSL/TLS Service Sends Client Certificate Request, But Does Not Require Client Certificates	Info	0.00	Pass	
21	199.48.239.47 (www.rosesandherbs.com)	SSLv2, SSLv3 and TLS v1.0 Vulnerable to CBC Attacks via chosen-plaintext (BEAST), CVE-2011-3389	Info	0.00	Pass	**NVD CVSS Score:** 4.30 **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:

#	IP Address	Vulnerabilities Noted	Severity	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
						N/C:N/I:N/A:N, with a base score of 0.0.
22	199.48.239.47 (www.rosesandherbs.com)	Wildcard SSL Certificate Detected	Info	0.00	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.
- Restrict access to any files, applications, and/or network services for which there is no business requirement to be publicly accessible.
- Configure the SSL service(s) running on this host to adhere to information security best practices.
- Upgrade and/or install security updates for Microsoft FrontPage Server Extensions.
- Ensure that any web applications running on this host is configured following industry security best practices.
- 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
No Special Notes					

Vulnerability Scan Report: Vulnerability Details

Part 1. Scan Information

Scan Customer Company	ANTIQUE ROSE AND HERB FARM	Date Scan Completed	2016-12-07
ASV Company	Trustwave Holdings, Inc.	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	199.48.239.47 (www.rosesandherbs.com)	rosesandherbs.com	Linux Kernel	true	tcp/21	ftp	proftpd:proftpd	220 ProFTPD 1.3.5b Server (ProFTPD) [199.48.239.47]
					tcp/25	smtp	postfix:postfix	220 web010.mivamerchant.net ESMTP

Vulnerability Scan Report: Vulnerability Details

#	Device	Names	OS	Ping	Service Information			
					Port	Protocol	Application	Detail
					tcp/80	http	apache:http_server	Apache
					tcp/443	http	apache:http_server	Apache
					tcp/465	smtp	postfix:postfix	220 web010.mivamerchant.net ESMTP
					tcp/587	smtp	postfix:postfix	220 web010.mivamerchant.net ESMTP

Vulnerability Scan Report: Vulnerability Details

#	Device	Names	OS	Ping	Service Information			
					Port	Protocol	Application	Detail
					tcp/993	imap	double_precision_incorporated:courier-imap	* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA AUTH=CRAM-MD5 AUTH=CRAM-SHA1 AUTH=CRAM-SHA256 AUTH=PLAIN IDLE ACL ACL2=UNION] Courier-IMAP ready. Copyright 1998-2015 Double Precision, Inc. See COPYING for distribution information.
					tcp/995	pop3		+OK Hello there. <28878.1481114357@localhost.localdomain>
					tcp/8443	http		sw-cp-server

#	Device	Names	OS	Ping	Service Information			
					Port	Protocol	Application	Detail
					tcp/8880	http		sw-cp-server
					udp/123	ntp		
					All other scanned ports were closed.			
2	71.49.118.68 (office)	fl-71-49-118-68.dhcp.embarqhsd.net		true				

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	63.210.67.31	ns1.myecommercedns.net	Discovered hosts using second-level domain name(s): rosesandherbs.com

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
2	63.210.67.32	ns2.myecommercedns.com	Discovered hosts using second-level domain name(s): rosesandherbs.com
3	199.48.239.47	mail.rosesandherbs.com	Discovered hosts using second-level domain name(s): rosesandherbs.com
4	208.77.55.4	ns1.myecommercedns.com	Discovered hosts using second-level domain name(s): rosesandherbs.com
5	208.77.55.254	ns2.myecommercedns.net	Discovered hosts using second-level domain name(s): rosesandherbs.com

Part 3c. Load Balancers

If you are using load balancers in your network to spread 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.

Vulnerability Scan Report: Vulnerability Details

Part 4. Vulnerability & 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.

199.48.239.47 (www.rosesandherbs.com)

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
1		Basic Authentication over HTTP	6.10	Medium	Fail	**Port:** tcp/80 This web service supports the use of basic authentication, which is a form of reversible encryption, over HTTP with is also not encrypted. **CVSSv2:** AV:A/AC:L/Au:N/C:C/I:N/A:N **Service:** apache:http_server **Evidence:**

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: http://www.rosesandherbs.com:80/_private/ WWW-Authenticate Header: Basic realm="www.rosesandherbs.com" **Remediation:** Migrate the service to HTTPS-only or deploy a stronger encryption scheme for credentials passed to this service over a clear text protocol.
2		TLSv1.0 Supported	5.00	Medium	Fail	**Port:** tcp/443 This service supports the use of the TLSv1.0 protocol. The TLSv1.0 protocol has known cryptographic weaknesses that can lead to the compromise of sensitive data within an encrypted session. Additionally, the PCI SSC and NIST have determined that the TLSv1.0 protocol no longer meets the definition of strong cryptography. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:P/A:N **Service:** apache:http_server **Reference:** https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf https://www.pcisecuritystandards.org/pdfs/15_04_15%20PCI%20DSS%203%201%20Press%20Release.pdf https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-FAQ-for-PCI-Manager-Customers/ https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-FAQ-for-TVM-Customers/ https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-Risk-Plan-of-Service-Provider-Template/ https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-Risk-

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Plan-Template/ https://www.trustwave.com/Resources/SpiderLabs-Blog/Bring-Out-Your-Dead--An-Update-on-the-PCI-relevance-of-SSLv3/?page=1&year=0&month=0 **Evidence:** Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA **Remediation:** Per the authorization of the PCI DSS, please dispute this finding and submit your Risk Mitigation & Migration Plan, which will grant you an EXCEPTION to this finding until June 30th, 2018. The Risk Mitigation & Migration Plan template can be found at the following link: https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-Risk-Plan-Template/ (you can copy/paste this link to your browser). Once you complete this plan, please use the 'Documents' tab of your TrustKeeper Portal account and upload your Risk Mitigation and Migration plan. Then, please dispute this finding within the Portal, stating that the Risk Mitigation and Migration plan has been uploaded to the TrustKeeper Portal. If you do not have access to the 'Documents' tab, please email support (support@trustwave.com) your organization's Risk Mitigation and Migration plan. You will then receive a confirmation email containing a reference number. This reference number should be placed in the resubmitted dispute. AFTER June 30th, 2018, the server should be configured to disable the use of the TLSv1.0 protocol in favor of cryptographically stronger protocols such as TLSv1.1 and TLSv1.2. For services that already support TLSv1.1 or TLSv1.2, simply disabling

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						the use of the TLSv1.0 protocol on this service is sufficient to address this finding. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
3		TLSv1.0 Supported	5.00	Medium	Fail	**Port:** tcp/465 This service supports the use of the TLSv1.0 protocol. The TLSv1.0 protocol has known cryptographic weaknesses that can lead to the compromise of sensitive data within an encrypted session. Additionally, the PCI SSC and NIST have determined that the TLSv1.0 protocol no longer meets the definition of strong cryptography. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:P/A:N **Service:** postfix:postfix **Reference:** https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf https://www.pcisecuritystandards.org/pdfs/15_04_15%20PCI%20DSS%203%201%20Press%20Release.pdf https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-FAQ-for-PCI-Manager-Customers/ https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-FAQ-for-TVM-Customers/ https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-Risk-Plan-of-Service-Provider-Template/ https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-Risk-Plan-Template/ https://www.trustwave.com/Resources/SpiderLabs-Blog/Bring-Out-Your-

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Dead--An-Update-on-the-PCI-relevance-of-SSLv3/?page=1&year=0&month=0 **Evidence:** Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA **Remediation:** Per the authorization of the PCI DSS, please dispute this finding and submit your Risk Mitigation & Migration Plan, which will grant you an EXCEPTION to this finding until June 30th, 2018. The Risk Mitigation & Migration Plan template can be found at the following link: https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-Risk-Plan-Template/ (you can copy/paste this link to your browser). Once you complete this plan, please use the 'Documents' tab of your TrustKeeper Portal account and upload your Risk Mitigation and Migration plan. Then, please dispute this finding within the Portal, stating that the Risk Mitigation and Migration plan has been uploaded to the TrustKeeper Portal. If you do not have access to the 'Documents' tab, please email support (support@trustwave.com) your organization's Risk Mitigation and Migration plan. You will then receive a confirmation email containing a reference number. This reference number should be placed in the resubmitted dispute. AFTER June 30th, 2018, the server should be configured to disable the use of the TLSv1.0 protocol in favor of cryptographically stronger protocols such as TLSv1.1 and TLSv1.2. For services that already support TLSv1.1 or TLSv1.2, simply disabling the use of the TLSv1.0 protocol on this service is sufficient to address this finding. Please note the port associated with this finding. This

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						finding may NOT be originating from port 443, which is what most online testing tools check by default.
4		TLSv1.0 Supported	5.00	Medium	Fail	**Port:** tcp/993 This service supports the use of the TLSv1.0 protocol. The TLSv1.0 protocol has known cryptographic weaknesses that can lead to the compromise of sensitive data within an encrypted session. Additionally, the PCI SSC and NIST have determined that the TLSv1.0 protocol no longer meets the definition of strong cryptography. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:P/A:N **Service:** double_precision_incorporated:courier-imap **Reference:** https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf https://www.pcisecuritystandards.org/pdfs/15_04_15%20PCI%20DSS%203%201%20Press%20Release.pdf https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-FAQ-for-PCI-Manager-Customers/ https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-FAQ-for-TVM-Customers/ https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-Risk-Plan-of-Service-Provider-Template/ https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-Risk-Plan-Template/ https://www.trustwave.com/Resources/SpiderLabs-Blog/Bring-Out-Your-Dead--An-Update-on-the-PCI-relevance-of-SSLv3/?page=1&year=0&month=0

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Evidence: Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA **Remediation:** Per the authorization of the PCI DSS, please dispute this finding and submit your Risk Mitigation & Migration Plan, which will grant you an EXCEPTION to this finding until June 30th, 2018. The Risk Mitigation & Migration Plan template can be found at the following link: https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-Risk-Plan-Template/ (you can copy/paste this link to your browser). Once you complete this plan, please use the 'Documents' tab of your TrustKeeper Portal account and upload your Risk Mitigation and Migration plan. Then, please dispute this finding within the Portal, stating that the Risk Mitigation and Migration plan has been uploaded to the TrustKeeper Portal. If you do not have access to the 'Documents' tab, please email support (support@trustwave.com) your organization's Risk Mitigation and Migration plan. You will then receive a confirmation email containing a reference number. This reference number should be placed in the resubmitted dispute. AFTER June 30th, 2018, the server should be configured to disable the use of the TLSv1.0 protocol in favor of cryptographically stronger protocols such as TLSv1.1 and TLSv1.2. For services that already support TLSv1.1 or TLSv1.2, simply disabling the use of the TLSv1.0 protocol on this service is sufficient to address this finding. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
5		TLSv1.0 Supported	5.00	Medium	Fail	**Port:** tcp/995 This service supports the use of the TLSv1.0 protocol. The TLSv1.0 protocol has known cryptographic weaknesses that can lead to the compromise of sensitive data within an encrypted session. Additionally, the PCI SSC and NIST have determined that the TLSv1.0 protocol no longer meets the definition of strong cryptography. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:P/A:N **Service:** pop3 **Reference:** https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf https://www.pcisecuritystandards.org/pdfs/15_04_15%20PCI%20DSS%203%201%20Press%20Release.pdf https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-FAQ-for-PCI-Manager-Customers/ https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-FAQ-for-TVM-Customers/ https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-Risk-Plan-of-Service-Provider-Template/ https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-Risk-Plan-Template/ https://www.trustwave.com/Resources/SpiderLabs-Blog/Bring-Out-Your-Dead--An-Update-on-the-PCI-relevance-of-SSLv3/?page=1&year=0&month=0 **Evidence:**

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA **Remediation:** Per the authorization of the PCI DSS, please dispute this finding and submit your Risk Mitigation & Migration Plan, which will grant you an EXCEPTION to this finding until June 30th, 2018. The Risk Mitigation & Migration Plan template can be found at the following link: https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-Risk-Plan-Template/ (you can copy/paste this link to your browser). Once you complete this plan, please use the 'Documents' tab of your TrustKeeper Portal account and upload your Risk Mitigation and Migration plan. Then, please dispute this finding within the Portal, stating that the Risk Mitigation and Migration plan has been uploaded to the TrustKeeper Portal. If you do not have access to the 'Documents' tab, please email support (support@trustwave.com) your organization's Risk Mitigation and Migration plan. You will then receive a confirmation email containing a reference number. This reference number should be placed in the resubmitted dispute. AFTER June 30th, 2018, the server should be configured to disable the use of the TLSv1.0 protocol in favor of cryptographically stronger protocols such as TLSv1.1 and TLSv1.2. For services that already support TLSv1.1 or TLSv1.2, simply disabling the use of the TLSv1.0 protocol on this service is sufficient to address this finding. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
6		TLSv1.0 Supported	5.00	Medium	Fail	**Port:** tcp/8443 This service supports the use of the TLSv1.0 protocol. The TLSv1.0 protocol has known cryptographic weaknesses that can lead to the compromise of sensitive data within an encrypted session. Additionally, the PCI SSC and NIST have determined that the TLSv1.0 protocol no longer meets the definition of strong cryptography. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:P/A:N **Service:** http **Reference:** https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf https://www.pcisecuritystandards.org/pdfs/15_04_15%20PCI%20DSS%203%201%20Press%20Release.pdf https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-FAQ-for-PCI-Manager-Customers/ https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-FAQ-for-TVM-Customers/ https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-Risk-Plan-of-Service-Provider-Template/ https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-Risk-Plan-Template/ https://www.trustwave.com/Resources/SpiderLabs-Blog/Bring-Out-Your-Dead--An-Update-on-the-PCI-relevance-of-SSLv3/?page=1&year=0&month=0 **Evidence:** Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1 : DHE-RSA-CAMELLIA256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : CAMELLIA256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : DHE-RSA-CAMELLIA128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : CAMELLIA128-SHA Cipher Suite: TLSv1 : ECDHE-RSA-DES-CBC3-SHA Cipher Suite: TLSv1 : EDH-RSA-DES-CBC3-SHA Cipher Suite: TLSv1 : DES-CBC3-SHA **Remediation:** Per the authorization of the PCI DSS, please dispute this finding and submit your Risk Mitigation & Migration Plan, which will grant you an EXCEPTION to this finding until June 30th, 2018. The Risk Mitigation & Migration Plan template can be found at the following link: https://www.trustwave.com/Resources/Library/Documents/PCI-3-1-Risk-Plan-Template/ (you can copy/paste this link to your browser). Once you complete this plan, please use the 'Documents' tab of your TrustKeeper Portal account and upload your Risk Mitigation and Migration plan. Then, please dispute this finding within the Portal, stating that the Risk Mitigation and Migration plan has been uploaded to the TrustKeeper Portal. If you do not have access to the 'Documents' tab, please email support (support@trustwave.com) your organization's Risk Mitigation and Migration plan. You will then receive a confirmation email containing a reference number. This reference number should be placed in the resubmitted dispute. AFTER June 30th, 2018, the server should be configured to disable the use of the TLSv1.0 protocol in favor of cryptographically stronger protocols such as TLSv1.1 and TLSv1.2. For services that already support TLSv1.1 or TLSv1.2, simply disabling the use of the TLSv1.0 protocol on this service is sufficient to address

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						this finding. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
7	CVE-2016-2183	Block cipher algorithms with block size of 64 bits (like DES and 3DES) birthday attack known as Sweet32	5.00	Medium	Fail	**Port:** tcp/8443 This is a cipher vulnerability, not limited to any specific SSL/TLS software implementation. DES and Tripple DES (3DES) block ciphers with a block size of 64 bits, have a birthday bound of approximately 4 billion blocks (or 2 to the power of 32, hence the name of this vulnerability). A man-in-the-middle (MitM) attacker, who is able to capture a large amount of encrypted network traffic, can recover sensitive plain text data. **CVE:** CVE-2016-2183 **NVD:** CVE-2016-2183 **CVSSv2:** AV:N/AC:L/Au:N/C:P/I:N/A:N **Service:** http **Reference:** https://access.redhat.com/security/cve/cve-2016-2183 https://sweet32.info/ https://www.openssl.org/blog/blog/2016/08/24/sweet32/ **Evidence:** Cipher Suite: TLSv1 : ECDHE-RSA-DES-CBC3-SHA Cipher Suite: TLSv1 : EDH-RSA-DES-CBC3-SHA Cipher Suite: TLSv1 : DES-CBC3-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-DES-CBC3-SHA Cipher Suite: TLSv1_1 : EDH-RSA-DES-CBC3-SHA

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1_1 : DES-CBC3-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-DES-CBC3-SHA Cipher Suite: TLSv1_2 : EDH-RSA-DES-CBC3-SHA Cipher Suite: TLSv1_2 : DES-CBC3-SHA **Remediation:** This issue can by avoided by disabling block ciphers of 64 bit length (like DES/3DES) in all the SSL/TLS servers. Exact procedure depends on the actual implementation. Please refer to the documentation of your SSL/TLS server software and actual service software (http server, mail server, etc). NOTE 1: This finding is based on a live test that actually detects which ciphers are supported by the server. It is very important to note that in many cases, a software update (backported version provided by Operating System vendor or "vanilla" release taken directly from SSL/TLS vendor) won't be enough to resolve this issue. Usually software update doesn't overwrite manually tweaked configuration files, which means, DES/3DES can be still available, even if the software update disables them by default. NOTE 2: On Windows 7/10 systems running RDP (Remote Desktop Protocol), the vulnerable cipher that should be disabled is labeled 'TLS_RSA_WITH_3DES_EDE_CBC_SHA'. NOTE 3: If disabling 64 bit block ciphers is not possible, please limit the number of requests client can make in a single TLS session and / or the keep-alive timeout value. As stated before, successful attack requires huge amounts of data gathered in a single TLS session (without rekeying).

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
8		Web Application Transmits Login Credentials Without Encryption	4.60	Medium	Fail	**Port:** tcp/80 There is a web application running on this host that transmits login credentials over HTTP, which is a clear-text protocol. As such, if an attacker was able to intercept traffic containing login credentials, it would be trivial to view user account and password information. **CVSSv2:** AV:A/AC:H/Au:N/C:C/I:N/A:N **Service:** apache:http_server **Evidence:** Protected Webpage: http://www.rosesandherbs.com/_private/ Authentication Type: basic **Remediation:** All web application communications containing sensitive information should be transmitted using SSL/TLS (HTTPS). If re-direction from HTTP to HTTPS is utilized in an attempt to remediate this finding, please ensure that such redirection occurs on the server side of the system (for example via the use of the HTTP "Location" header element) and that redirection is not reliant upon the client (browser) side.
9		No X-FRAME-OPTIONS Header	2.60	Low	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).

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						CVSSv2: AV:N/AC:H/Au:N/C:N/I:P/A:N **Service:** apache:http_server **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.
10		No X-FRAME-OPTIONS Header	2.60	Low	Pass	**Port:** tcp/443 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:H/Au:N/C:N/I:P/A:N **Service:** apache:http_server **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.

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
11		SSL Certificate is Not Trusted	0.00	Info	Pass	**Port:** tcp/21 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:** proftpd:proftpd **Evidence:** Subject: /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Reason: The hostname on the certificate does not match any of the hostnames provided to the scanner. Reason: One or more certificates in the chain cannot be validated. **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. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
12		Wildcard SSL Certificate	0.00	Info	Pass	**Port:** tcp/21

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
		Detected				An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** proftpd:proftpd **Evidence:** Subject: /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Wildcard Subject Name: *.mivamerchant.net **Remediation:** Review your certificate configurations to assure that wildcard certificates are suitable for your application.
13		SSL Certificate Common Name Does Not Validate	0.00	Info	Pass	**Port:** tcp/21 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:** proftpd:proftpd **Evidence:**

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Subject: /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Hostnames provided to scanner: www.rosesandherbs.com, 199.48.239.47 Subject Name: *.mivamerchant.net Subject Alternative Name: *.mivamerchant.net Subject Alternative Name: mivamerchant.net **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. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
14		SSL Certificate Chain Not Trusted	0.00	Info	Pass	**Port:** tcp/21 An SSL certificate in the certificate chain does not validate with a well-known Certificate Authority (CA). Users may receive a security warning when using this service. The certificate chain includes all intermediary certificates, in addition to the root certificate, that is used to validate your certificate. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** proftpd:proftpd **Evidence:**

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Subject: /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Reason: The certificate's issuer certificate could not be identified. Reason: Errors in the certificate chain prevent the certificate from being verified. **Remediation:** Ensure that intermediary certificates that are provided via the SSL service are the correct ones, and that they have not been revoked or expired. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
15		SSL/TLS Service Sends Client Certificate Request, But Does Not Require Client Certificates	0.00	Info	Pass	**Port:** tcp/21 The service is protected using the SSL/TLS protocol, and appears to be configured incorrectly. When an SSL client connects, the SSL service on the remote host sends a Certificate Request message, indicating that it would like to receive an SSL certificate from the client for authentication purposes. Normally, an SSL client is not required to provide a certificate, as most servers are not concerned with authenticating clients at the network level. However, in the case of this SSL server, it is still possible to negotiate SSL without providing a client certificate. Normally, when a server sends a Certificate Request to a client, it will not negotiate SSL without the client providing a valid certificate. This is akin to prompting for a password, but allowing anyone in if no password is provided. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Service: proftpd:proftpd **Remediation:** This may represent a failing in the configuration of the SSL service. If it is not intended that SSL clients have access without providing a client certificate, then the SSL server's configuration may need to be corrected.
16		FTP Server Supports AUTH TLS (STARTTLS)	0.00	Info	Pass	**Port:** tcp/21 The FTP service running on this host supports encryption using the AUTH TLS command. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** proftpd:proftpd **Reference:** http://en.wikipedia.org/wiki/STARTTLS **Evidence:** Message: 234 AUTH TLS successful **Remediation:** No remediation necessary. This is identified for informational purposes.
17		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 not be trusted. Users may receive a security warning when using this service. This occurs because either the certificate or a certificate in its

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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:** postfix:postfix **Evidence:** Subject: /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Reason: The hostname on the certificate does not match any of the hostnames provided to the scanner. **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. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
18		Wildcard SSL Certificate Detected	0.00	Info	Pass	**Port:** tcp/25 An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** postfix:postfix

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Evidence: Subject: /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Wildcard Subject Name: *.mivamerchant.net **Remediation:** Review your certificate configurations to assure that wildcard certificates are suitable for your application.
19		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:** postfix:postfix **Evidence:** Subject: /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Hostnames provided to scanner: www.rosesandherbs.com,

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						199.48.239.47 Subject Name: *.mivamerchant.net Subject Alternative Name: *.mivamerchant.net Subject Alternative Name: mivamerchant.net **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. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
20		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 **Service:** postfix:postfix **Evidence:** Message: 220 2.0.0 Ready to start TLS **Remediation:** No remediation necessary. This is identified for informational purposes.
21		FrontPage Detected	0.00	Info	Pass	**Port:** tcp/80

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Microsoft FrontPage extensions were detected on this web server. This module provides remote authoring capabilities and requires that proper permissions be set in order to prevent unauthorized editing of site content. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** apache:http_server **Remediation:** This test does not detect if there are problems with your configuration; however, due to the high number of attacks which utilize FrontPage, we recommend that you double check that proper authentication is required to access the administrative and authoring functions.
22		Discovered HTTP Methods	0.00	Info	Pass	**Port:** tcp/80 Requesting the allowed HTTP OPTIONS from this host shows which HTTP protocol methods are supported by its web server. Note that, in some cases, this information is not reported by the web server accurately. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** apache:http_server **Evidence:** URL: http://www.rosesandherbs.com/ Methods: GET, HEAD, POST, OPTIONS **Remediation:**

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Review your web server configuration and ensure that only those HTTP methods required for your business operations are enabled.
23		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:** apache:http_server **Evidence:** URL: http://www.rosesandherbs.com:80/_private/ HTTP Response Code: 401 URL: http://www.rosesandherbs.com:80/images/ HTTP Response Code: 200 URL: http://www.rosesandherbs.com:80/webstat/ HTTP Response Code: 301 **Remediation:** Review these directories and verify that there is no unintentional content made available to remote users.
24		Protected Web Page	0.00	Info	Pass	**Port:** tcp/80 The web server requires authentication for some resources. Several authentication types are available such as: 1) Basic is the most simplistic and sends credentials in clear text 2) NTLM can be used for single sign on in a Microsoft environment, but it cannot be used on

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						both a proxy and the web server 3) Digest is a cryptographically strong scheme but credentials can still be brute forced or discovered through dictionary attacks. Note that this list is limited to ten instances of this finding. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** apache:http_server **Evidence:** Protected Webpage: http://www.rosesandherbs.com/_private/ Authentication Type: basic Authentication Realm: realm="www.rosesandherbs.com" **Remediation:** Confirm that the authentication in use is appropriate.
25		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:** apache:http_server **Reference:** http://packetstormsecurity.org/files/view/71358/appOSfingerprint.txt **Evidence:** Potential Operating System: Unix/Linux

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: There is no solution at this time.
26		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/80 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:** apache:http_server **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: http://www.rosesandherbs.com/contact.htm

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	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.
27		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/80 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:** apache:http_server **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: http://www.rosesandherbs.com/definitions/usdazones.htm **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.
28		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/80 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:** apache:http_server

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	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: http://www.rosesandherbs.com/fairytale.htm **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.
29		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/80 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.

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** apache:http_server **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: http://www.rosesandherbs.com/mm5/merchant.mvc **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.
30		HTTP Responses Missing Character Encoding	0.00	Info	Pass	**Port:** tcp/80 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

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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:** apache:http_server **Reference:** http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection http://wiki.whatwg.org/wiki/Web_Encodings **Evidence:** URL: http://www.rosesandherbs.com/unsubscribe.htm **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.
31		SSL Perfect Forward Secrecy Supported	0.00	Info	Pass	**Port:** tcp/443 The server supports Ephemeral Diffie-Hellman ciphers for the SSL/TLS key exchange phase. Using this algorithm enforces Forward Secrecy for secure communications with the server. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** apache:http_server

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Evidence: Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA **Remediation:** No remediation is necessary.
32		SSL Certificate is Not Trusted	0.00	Info	Pass	**Port:** tcp/443 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:** apache:http_server **Evidence:**

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Subject: /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Reason: The hostname on the certificate does not match any of the hostnames provided to the scanner. Reason: One or more certificates in the chain cannot be validated. **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. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
33		Wildcard SSL Certificate Detected	0.00	Info	Pass	**Port:** tcp/443 An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** apache:http_server **Evidence:** Subject: /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Wildcard Subject Name: *.mivamerchant.net

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: Review your certificate configurations to assure that wildcard certificates are suitable for your application.
34		SSL Certificate Common Name Does Not Validate	0.00	Info	Pass	**Port:** tcp/443 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:** apache:http_server **Evidence:** Subject: /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Hostnames provided to scanner: www.rosesandherbs.com, 199.48.239.47 Subject Name: *.mivamerchant.net Subject Alternative Name: *.mivamerchant.net Subject Alternative Name: mivamerchant.net **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

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
35		SSL Certificate Chain Not Trusted	0.00	Info	Pass	**Port:** tcp/443 An SSL certificate in the certificate chain does not validate with a well-known Certificate Authority (CA). Users may receive a security warning when using this service. The certificate chain includes all intermediary certificates, in addition to the root certificate, that is used to validate your certificate. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** apache:http_server **Evidence:** Subject: /C=US/O=GeoTrust Inc./CN=GeoTrust Global CA Issuer: /C=US/O=Equifax/OU=Equifax Secure Certificate Authority Certificate Chain Depth: 2 Reason: The certificate's issuer certificate could not be identified. **Remediation:** Ensure that intermediary certificates that are provided via the SSL service are the correct ones, and that they have not been revoked or expired. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
36	CVE-2011-3389	SSLv2, SSLv3 and TLS v1.0 Vulnerable to CBC Attacks via chosen-plaintext (BEAST)	0.00	Info	Pass	**Port:** tcp/443 This server supports a version of SSL vulnerable to a Cipher Block Chaining (CBC) attack. When using a block-based cipher with SSLv2, SSLv3 or TLS v1.0, it is possible to perform a cryptographic attack called a chosen-plaintext attack. 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 an attacker to decrypt the SSL/TLS connection to gain access to sensitive information. Although, the BEAST attack is the only known exploit, other services not related to web servers (e.g. IMAP) may also be vulnerable to such attack. **CVE:** CVE-2011-3389 **NVD:** CVE-2011-3389 **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** apache:http_server **Reference:** http://httpd.apache.org/docs/trunk/mod/mod_ssl.html#sslciphersuite http://support.microsoft.com/kb/2643584 http://technet.microsoft.com/en-us/security/advisory/2588513 **Evidence:** Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: The server should be configured to allow only TLS versions 1.1 and 1.2, which are not vulnerable to this CBC attack. Although the latest versions of all major web browsers support TLS 1.1 and 1.2 enabled by default, disabling previous versions may prevent other services than HTTP from connecting to the server if they do not support these versions of TLS.
37		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	**Port:** tcp/443 The finding reports the SSL cipher suites for each SSL/TLS service version provided by the remote service. This finding does not represent a vulnerability, but is only meant to provide visibility into the behavior and configuration of the remote SSL/TLS service. The information provided as part of this finding includes the SSL version (ex: TLSv1) as well as the name of the cipher suite (ex: RC4-SHA). A cipher suite is a set of cryptographic algorithms that provide authentication, encryption, and message authentication code (MAC) as part of an SSL/TLS negotiation and through the lifetime of the SSL session. It is typical that an SSL service would support multiple cipher suites. A cipher suite can be supported by across multiple SSL/TLS versions, so you should be of no concern to see the same cipher name reported for multiple **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** apache:http_server **Reference:** http://www.openssl.org/docs/apps/ciphers.html

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Evidence: Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : AES256-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : AES128-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : AES256-SHA256 Cipher Suite: TLSv1_2 : AES256-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1_2 : AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA **Remediation:** No remediation is necessary.
38		SSL Perfect Forward Secrecy Supported	0.00	Info	Pass	**Port:** tcp/465 The server supports Ephemeral Diffie-Hellman ciphers for the SSL/TLS key exchange phase. Using this algorithm enforces Forward Secrecy for secure communications with the server. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** postfix:postfix **Evidence:** Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA **Remediation:**

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						No remediation is necessary.
39		SSL Certificate is Not Trusted	0.00	Info	Pass	**Port:** tcp/465 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:** postfix:postfix **Evidence:** Subject: /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Reason: The hostname on the certificate does not match any of the hostnames provided to the scanner. **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. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
40		Wildcard SSL Certificate Detected	0.00	Info	Pass	**Port:** tcp/465 An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** postfix:postfix **Evidence:** Subject: /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Wildcard Subject Name: *.mivamerchant.net **Remediation:** Review your certificate configurations to assure that wildcard certificates are suitable for your application.
41		SSL Certificate Common Name Does Not Validate	0.00	Info	Pass	**Port:** tcp/465 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:** postfix:postfix

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Evidence: Subject: /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Hostnames provided to scanner: www.rosesandherbs.com, 199.48.239.47 Subject Name: *.mivamerchant.net Subject Alternative Name: *.mivamerchant.net Subject Alternative Name: mivamerchant.net **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. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
42	CVE-2011-3389	SSLv2, SSLv3 and TLS v1.0 Vulnerable to CBC Attacks via chosen-plaintext (BEAST)	0.00	Info	Pass	**Port:** tcp/465 This server supports a version of SSL vulnerable to a Cipher Block Chaining (CBC) attack. When using a block-based cipher with SSLv2, SSLv3 or TLS v1.0, it is possible to perform a cryptographic attack called a chosen-plaintext attack. 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 an attacker to decrypt the SSL/TLS connection to gain access to sensitive information. Although, the BEAST attack is

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						the only known exploit, other services not related to web servers (e.g. IMAP) may also be vulnerable to such attack. **CVE:** CVE-2011-3389 **NVD:** CVE-2011-3389 **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** postfix:postfix **Reference:** http://httpd.apache.org/docs/trunk/mod/mod_ssl.html#sslciphersuite http://support.microsoft.com/kb/2643584 http://technet.microsoft.com/en-us/security/advisory/2588513 **Evidence:** Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA **Remediation:** The server should be configured to allow only TLS versions 1.1 and 1.2, which are not vulnerable to this CBC attack. Although the latest versions of all major web browsers support TLS 1.1 and 1.2 enabled by default, disabling previous versions may prevent other services than HTTP from connecting to the server if they do not support these versions of TLS.

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
43		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	**Port:** tcp/465 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:** postfix:postfix **Reference:** http://www.openssl.org/docs/apps/ciphers.html **Evidence:** Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1_1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : AES256-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : AES128-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : AES256-SHA256 Cipher Suite: TLSv1_2 : AES256-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA **Remediation:** No remediation is necessary.

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
44		SSL Certificate is Not Trusted	0.00	Info	Pass	**Port:** tcp/587 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:** postfix:postfix **Evidence:** Subject: /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Reason: The hostname on the certificate does not match any of the hostnames provided to the scanner. **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. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
45		Wildcard SSL Certificate Detected	0.00	Info	Pass	**Port:** tcp/587 An SSL certificate with a wildcarded common name (CN) record (e.g., *.

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						mydomain.com) was detected on this service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** postfix:postfix **Evidence:** Subject: /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Wildcard Subject Name: *.mivamerchant.net **Remediation:** Review your certificate configurations to assure that wildcard certificates are suitable for your application.
46		SSL Certificate Common Name Does Not Validate	0.00	Info	Pass	**Port:** tcp/587 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:** postfix:postfix **Evidence:** Subject: /C=US/ST=California/L=San Diego/O=Miva Merchant Inc.

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						/CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Hostnames provided to scanner: www.rosesandherbs.com, 199.48.239.47 Subject Name: *.mivamerchant.net Subject Alternative Name: *.mivamerchant.net Subject Alternative Name: mivamerchant.net **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. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
47		SMTP Service Supports the STARTTLS Command	0.00	Info	Pass	**Port:** tcp/587 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 **Service:** postfix:postfix **Evidence:** Message: 220 2.0.0 Ready to start TLS **Remediation:**

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						No remediation necessary. This is identified for informational purposes.
48		SSL Perfect Forward Secrecy Supported	0.00	Info	Pass	**Port:** tcp/993 The server supports Ephemeral Diffie-Hellman ciphers for the SSL/TLS key exchange phase. Using this algorithm enforces Forward Secrecy for secure communications with the server. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** double_precision_incorporated:courier-imap **Evidence:** Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA **Remediation:** No remediation is necessary.
49		SSL Certificate is Not Trusted	0.00	Info	Pass	**Port:** tcp/993 It was not possible to validate the SSL certificate, and thus it could not

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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:** double_precision_incorporated:courier-imap **Evidence:** Subject: /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Reason: The hostname on the certificate does not match any of the hostnames provided to the scanner. **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. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
50		Wildcard SSL Certificate Detected	0.00	Info	Pass	**Port:** tcp/993 An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Service: double_precision_incorporated:courier-imap **Evidence:** Subject: /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Wildcard Subject Name: *.mivamerchant.net **Remediation:** Review your certificate configurations to assure that wildcard certificates are suitable for your application.
51		SSL Certificate Common Name Does Not Validate	0.00	Info	Pass	**Port:** tcp/993 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:** double_precision_incorporated:courier-imap **Evidence:** Subject: /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Hostnames provided to scanner: www.rosesandherbs.com, 199.48.239.47 Subject Name: *.mivamerchant.net Subject Alternative Name: *.mivamerchant.net Subject Alternative Name: mivamerchant.net **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. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
52	CVE-2011-3389	SSLv2, SSLv3 and TLS v1.0 Vulnerable to CBC Attacks via chosen-plaintext (BEAST)	0.00	Info	Pass	**Port:** tcp/993 This server supports a version of SSL vulnerable to a Cipher Block Chaining (CBC) attack. When using a block-based cipher with SSLv2, SSLv3 or TLS v1.0, it is possible to perform a cryptographic attack called a chosen-plaintext attack. 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 an attacker to decrypt the SSL/TLS connection to gain access to sensitive information. Although, the BEAST attack is the only known exploit, other services not related to web servers (e.g. IMAP) may also be vulnerable to such attack. **CVE:** CVE-2011-3389 **NVD:** CVE-2011-3389 **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Service: double_precision_incorporated:courier-imap **Reference:** http://httpd.apache.org/docs/trunk/mod/mod_ssl.html#sslciphersuite http://support.microsoft.com/kb/2643584 http://technet.microsoft.com/en-us/security/advisory/2588513 **Evidence:** Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA **Remediation:** The server should be configured to allow only TLS versions 1.1 and 1.2, which are not vulnerable to this CBC attack. Although the latest versions of all major web browsers support TLS 1.1 and 1.2 enabled by default, disabling previous versions may prevent other services than HTTP from connecting to the server if they do not support these versions of TLS.
53		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	**Port:** tcp/993 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

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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:** double_precision_incorporated:courier-imap **Reference:** http://www.openssl.org/docs/apps/ciphers.html **Evidence:** Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : AES256-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : AES128-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : AES256-SHA256 Cipher Suite: TLSv1_2 : AES256-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA **Remediation:** No remediation is necessary.
54		SSL Perfect Forward Secrecy Supported	0.00	Info	Pass	**Port:** tcp/995 The server supports Ephemeral Diffie-Hellman ciphers for the SSL/TLS key exchange phase. Using this algorithm enforces Forward Secrecy for secure communications with the server. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** pop3

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Evidence: Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA **Remediation:** No remediation is necessary.
55		SSL Certificate is Not Trusted	0.00	Info	Pass	**Port:** tcp/995 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:**

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Subject: /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Reason: The hostname on the certificate does not match any of the hostnames provided to the scanner. **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. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
56		Wildcard SSL Certificate Detected	0.00	Info	Pass	**Port:** tcp/995 An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** pop3 **Evidence:** Subject: /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Wildcard Subject Name: *.mivamerchant.net **Remediation:**

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Review your certificate configurations to assure that wildcard certificates are suitable for your application.
57		SSL Certificate Common Name Does Not Validate	0.00	Info	Pass	**Port:** tcp/995 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=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Hostnames provided to scanner: www.rosesandherbs.com, 199.48.239.47 Subject Name: *.mivamerchant.net Subject Alternative Name: *.mivamerchant.net Subject Alternative Name: mivamerchant.net **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

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						mapped to the correct IP address. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
58	CVE-2011-3389	SSLv2, SSLv3 and TLS v1.0 Vulnerable to CBC Attacks via chosen-plaintext (BEAST)	0.00	Info	Pass	**Port:** tcp/995 This server supports a version of SSL vulnerable to a Cipher Block Chaining (CBC) attack. When using a block-based cipher with SSLv2, SSLv3 or TLS v1.0, it is possible to perform a cryptographic attack called a chosen-plaintext attack. 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 an attacker to decrypt the SSL/TLS connection to gain access to sensitive information. Although, the BEAST attack is the only known exploit, other services not related to web servers (e.g. IMAP) may also be vulnerable to such attack. **CVE:** CVE-2011-3389 **NVD:** CVE-2011-3389 **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** pop3 **Reference:** http://httpd.apache.org/docs/trunk/mod/mod_ssl.html#sslciphersuite http://support.microsoft.com/kb/2643584 http://technet.microsoft.com/en-us/security/advisory/2588513 **Evidence:** Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA **Remediation:** The server should be configured to allow only TLS versions 1.1 and 1.2, which are not vulnerable to this CBC attack. Although the latest versions of all major web browsers support TLS 1.1 and 1.2 enabled by default, disabling previous versions may prevent other services than HTTP from connecting to the server if they do not support these versions of TLS.
59		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	**Port:** tcp/995 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

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : AES256-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : AES128-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : AES256-SHA256 Cipher Suite: TLSv1_2 : AES256-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA **Remediation:** No remediation is necessary.
60		SSL Perfect Forward Secrecy Supported	0.00	Info	Pass	**Port:** tcp/8443 The server supports Ephemeral Diffie-Hellman ciphers for the SSL/TLS key exchange phase. Using this algorithm enforces Forward Secrecy for secure communications with the server. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Evidence:** Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-CAMELLIA256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : DHE-RSA-CAMELLIA128-SHA Cipher Suite: TLSv1 : EDH-RSA-DES-CBC3-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-CAMELLIA256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES128-SHA

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1_1 : DHE-RSA-CAMELLIA128-SHA Cipher Suite: TLSv1_1 : EDH-RSA-DES-CBC3-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-CAMELLIA256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-CAMELLIA128-SHA Cipher Suite: TLSv1_2 : EDH-RSA-DES-CBC3-SHA **Remediation:** No remediation is necessary.
61		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 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=California/L=San Diego/O=Miva Merchant Inc.

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						/CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Reason: The hostname on the certificate does not match any of the hostnames provided to the scanner. Reason: One or more certificates in the chain cannot be validated. **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. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
62		Wildcard SSL Certificate Detected	0.00	Info	Pass	**Port:** tcp/8443 An SSL certificate with a wildcarded common name (CN) record (e.g., *.mydomain.com) was detected on this service. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Evidence:** Subject: /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Wildcard Subject Name: *.mivamerchant.net **Remediation:**

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Review your certificate configurations to assure that wildcard certificates are suitable for your application.
63		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=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 Certificate Chain Depth: 0 Hostnames provided to scanner: www.rosesandherbs.com, 199.48.239.47 Subject Name: *.mivamerchant.net Subject Alternative Name: *.mivamerchant.net Subject Alternative Name: mivamerchant.net **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

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						mapped to the correct IP address. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
64		SSL Certificate Chain Not Trusted	0.00	Info	Pass	**Port:** tcp/8443 An SSL certificate in the certificate chain does not validate with a well-known Certificate Authority (CA). Users may receive a security warning when using this service. The certificate chain includes all intermediary certificates, in addition to the root certificate, that is used to validate your certificate. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Evidence:** Subject: /C=US/O=GeoTrust Inc./CN=GeoTrust Global CA Issuer: /C=US/O=Equifax/OU=Equifax Secure Certificate Authority Certificate Chain Depth: 2 Reason: The certificate's issuer certificate could not be identified. **Remediation:** Ensure that intermediary certificates that are provided via the SSL service are the correct ones, and that they have not been revoked or expired. Please note the port associated with this finding. This finding may NOT be originating from port 443, which is what most online testing tools check by default.
65	CVE-2011-3389	SSLv2, SSLv3 and TLS v1.0	0.00	Info	Pass	**Port:** tcp/8443

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
		Vulnerable to CBC Attacks via chosen-plaintext (BEAST)				This server supports a version of SSL vulnerable to a Cipher Block Chaining (CBC) attack. When using a block-based cipher with SSLv2, SSLv3 or TLS v1.0, it is possible to perform a cryptographic attack called a chosen-plaintext attack. 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 an attacker to decrypt the SSL/TLS connection to gain access to sensitive information. Although, the BEAST attack is the only known exploit, other services not related to web servers (e.g. IMAP) may also be vulnerable to such attack. **CVE:** CVE-2011-3389 **NVD:** CVE-2011-3389 **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Reference:** http://httpd.apache.org/docs/trunk/mod/mod_ssl.html#sslciphersuite http://support.microsoft.com/kb/2643584 http://technet.microsoft.com/en-us/security/advisory/2588513 **Evidence:** Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : ECDHE-RSA-DES-CBC3-SHA Cipher Suite: TLSv1 : EDH-RSA-DES-CBC3-SHA Cipher Suite: TLSv1 : DES-CBC3-SHA

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: The server should be configured to allow only TLS versions 1.1 and 1.2, which are not vulnerable to this CBC attack. Although the latest versions of all major web browsers support TLS 1.1 and 1.2 enabled by default, disabling previous versions may prevent other services than HTTP from connecting to the server if they do not support these versions of TLS.
66		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 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:**

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						http://www.openssl.org/docs/apps/ciphers.html **Evidence:** Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1 : DHE-RSA-CAMELLIA256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : CAMELLIA256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1 : DHE-RSA-CAMELLIA128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : CAMELLIA128-SHA Cipher Suite: TLSv1 : ECDHE-RSA-DES-CBC3-SHA Cipher Suite: TLSv1 : EDH-RSA-DES-CBC3-SHA Cipher Suite: TLSv1 : DES-CBC3-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : DHE-RSA-CAMELLIA256-SHA Cipher Suite: TLSv1_1 : AES256-SHA Cipher Suite: TLSv1_1 : CAMELLIA256-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : DHE-RSA-CAMELLIA128-SHA Cipher Suite: TLSv1_1 : AES128-SHA Cipher Suite: TLSv1_1 : CAMELLIA128-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-DES-CBC3-SHA Cipher Suite: TLSv1_1 : EDH-RSA-DES-CBC3-SHA Cipher Suite: TLSv1_1 : DES-CBC3-SHA

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : DHE-RSA-CAMELLIA256-SHA Cipher Suite: TLSv1_2 : AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : AES256-SHA256 Cipher Suite: TLSv1_2 : AES256-SHA Cipher Suite: TLSv1_2 : CAMELLIA256-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : DHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : DHE-RSA-CAMELLIA128-SHA Cipher Suite: TLSv1_2 : AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA Cipher Suite: TLSv1_2 : CAMELLIA128-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-DES-CBC3-SHA Cipher Suite: TLSv1_2 : EDH-RSA-DES-CBC3-SHA Cipher Suite: TLSv1_2 : DES-CBC3-SHA **Remediation:** No remediation is necessary.

Vulnerability Scan Report: Vulnerability Details

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
67		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.rosesandherbs.com:8443/admin/ HTTP Response Code: 200 URL: https://www.rosesandherbs.com:8443/admin-console/ URL: https://www.rosesandherbs.com:8443/phpMyAdmin/ HTTP Response Code: 301 URL: https://www.rosesandherbs.com:8443/phpmyadmin/ URL: https://www.rosesandherbs.com:8443/admin.back/ URL: https://www.rosesandherbs.com:8443/admin_/ URL: https://www.rosesandherbs.com:8443/admin-bak/ URL: https://www.rosesandherbs.com:8443/administrator/ URL: https://www.rosesandherbs.com:8443/admin-old/ URL: https://www.rosesandherbs.com:8443/adminuser/ URL: https://www.rosesandherbs.com:8443/sitebuildercontent/ URL: https://www.rosesandherbs.com:8443/sitebuilderfiles/ URL: https://www.rosesandherbs.com:8443/sitebuilderpictures/ **Remediation:**

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Review these directories and verify that there is no unintentional content made available to remote users.
68		Discovered Web Directories	0.00	Info	Pass	**Port:** tcp/8880 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.rosesandherbs.com:8880/admin/ HTTP Response Code: 200 URL: http://www.rosesandherbs.com:8880/admin-console/ URL: http://www.rosesandherbs.com:8880/phpMyAdmin/ HTTP Response Code: 301 URL: http://www.rosesandherbs.com:8880/phpmyadmin/ URL: http://www.rosesandherbs.com:8880/admin.back/ URL: http://www.rosesandherbs.com:8880/admin_/ URL: http://www.rosesandherbs.com:8880/admin-bak/ URL: http://www.rosesandherbs.com:8880/administrator/ URL: http://www.rosesandherbs.com:8880/admin-old/ URL: http://www.rosesandherbs.com:8880/adminuser/ URL: http://www.rosesandherbs.com:8880/sitebuildercontent/ URL: http://www.rosesandherbs.com:8880/sitebuilderfiles/ URL: http://www.rosesandherbs.com:8880/sitebuilderpictures/

199.48.239.47 (www.rosesandherbs.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: Review these directories and verify that there is no unintentional content made available to remote users.
69		Enumerated Hostnames	0.00	Info	Pass	This list contains all hostnames discovered during the scan that are believed to belong to this host. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Evidence:** Hostname: web010.mivamerchant.net, Source: SMTP Protocol Hostname: mivamerchant.net, Source: SSL Certificate Subject subjectAltName DNS **Remediation:** No action is required.

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.

Vulnerability Scan Report: Vulnerability Details

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	199.48.239.47 (www.rosesandherbs.com)	rosesandherbs.com	tcp / 80	apache:http_server	
2	199.48.239.47 (www.rosesandherbs.com)	rosesandherbs.com	tcp / 443	apache:http_server	
3	199.48.239.47 (www.rosesandherbs.com)	rosesandherbs.com	tcp / 8443		
4	199.48.239.47 (www.rosesandherbs.com)	rosesandherbs.com	tcp / 8880		

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

Vulnerability Scan Report: Vulnerability Details

#	Service	Common Name	Expires	Details
1	199.48.239.47 : 21 (ftp) (www.rosesandherbs.com)	*.mivamerchant.net	2018-09-25 18:59	**Issued to:** /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net **Issued by:** /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 **Fingerprint:** 83:54:2E:D7:B0:FB:B2:DE:17:DC:08:6D:CC:C6:53:64
2	199.48.239.47 : 25 (smtp) (www.rosesandherbs.com)	*.mivamerchant.net	2018-09-25 18:59	**Issued to:** /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net **Issued by:** /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 **Fingerprint:** 83:54:2E:D7:B0:FB:B2:DE:17:DC:08:6D:CC:C6:53:64
3	199.48.239.47 : 443 (http) (www.rosesandherbs.com)	*.mivamerchant.net	2018-09-25 18:59	**Issued to:** /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net **Issued by:** /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 **Fingerprint:** 83:54:2E:D7:B0:FB:B2:DE:17:DC:08:6D:CC:C6:53:64
4	199.48.239.47 : 465 (smtp) (www.rosesandherbs.com)	*.mivamerchant.net	2018-09-25 18:59	**Issued to:** /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net **Issued by:** /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 **Fingerprint:** 83:54:2E:D7:B0:FB:B2:DE:17:DC:08:6D:CC:C6:53:64
5	199.48.239.47 : 587 (smtp) (www.rosesandherbs.com)	*.mivamerchant.net	2018-09-25 18:59	**Issued to:** /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net **Issued by:** /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 **Fingerprint:** 83:54:2E:D7:B0:FB:B2:DE:17:DC:08:6D:CC:C6:53:64
6	199.48.239.47 : 993 (imap) (www.rosesandherbs.com)	*.mivamerchant.net	2018-09-25 18:59	**Issued to:** /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net **Issued by:** /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3

#	Service	Common Name	Expires	Details
				Fingerprint: 83:54:2E:D7:B0:FB:B2:DE:17:DC:08:6D:CC:C6:53:64
7	199.48.239.47 : 995 (pop3) (www.rosesandherbs.com)	*.mivamerchant.net	2018-09-25 18:59	**Issued to:** /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net **Issued by:** /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 **Fingerprint:** 83:54:2E:D7:B0:FB:B2:DE:17:DC:08:6D:CC:C6:53:64
8	199.48.239.47 : 8443 (http) (www.rosesandherbs.com)	*.mivamerchant.net	2018-09-25 18:59	**Issued to:** /C=US/ST=California/L=San Diego/O=Miva Merchant Inc./CN=*.mivamerchant.net **Issued by:** /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3 **Fingerprint:** 83:54:2E:D7:B0:FB:B2:DE:17:DC:08:6D:CC:C6:53:64

Part 6. Disputed Vulnerability & 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
No disputes found that have been removed from the scoring of this report.				

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:	