Trustwave®

Report Date: 2017-11-16

Vulnerability Scan Report: Attestation of Compliance

Scan Customer Information				Approved Scanning Vendor Information			
Company Name:	SHOPPING CART ELITE			**Company Name:**	Trustwave Holdings, Inc.		
Contact:	Igor Soshkin	**Title:**		**Contact:**	Trustwave Support	**URL:**	www.trustwave.com
Telephone:	718-705-4886	**E-mail:**	igor@shoppingcartelite.com	**Telephone:**	1-800-363-1621	**E-mail:**	support@trustwave.com
Business Address:	718 3RD AVE 2ND FLOOR-B			**Business Address:**	70 West Madison St., Ste 1050		
City:	BROOKLYN	**State/Province:**	New York	**City:**	Chicago	**State/Province:**	IL
ZIP/Postal Code:	11232	**Country:**	US	**ZIP/Postal Code:**	60602	**Country:**	US

Scan Status

Pass	Scan Compliance Status
0	Number of unique components scanned that are in scope
0	Number of identified failing vulnerabilities
1	Number of components scanned by TrustKeeper but confirmed by the customer not to be in scope
2017-10-28	Date Scan Completed
2018-01-28	Scan Expiration Date (3 months from Date Scan Completed)

Scan Customer Attestation

SHOPPING CART ELITE 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. SHOPPING CART ELITE 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 SHOPPING CART ELITEs 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.

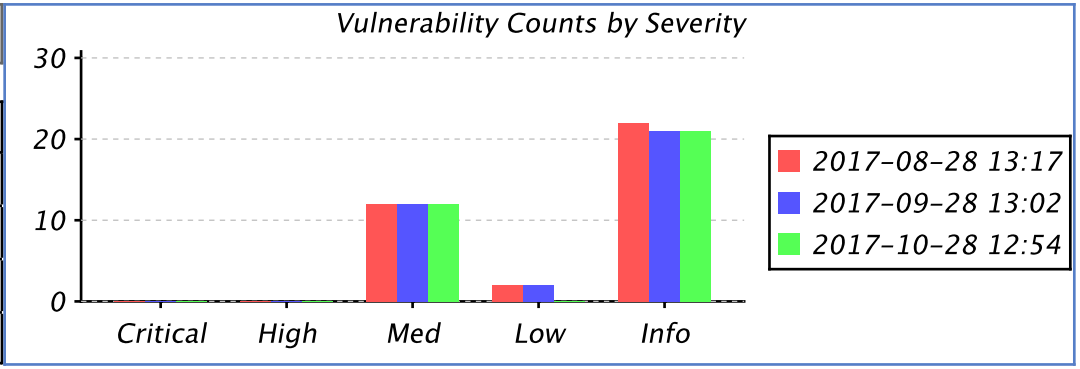
Trustwave attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, and 3) active interference. This report and any exceptions were reviewed by the Trustwave Quality Assurance Process.

Vulnerability Scan Report: Table of Contents

Vulnerability Scan Report: Executive Summary

Part 1. Scan Information

Scan Customer Company	SHOPPING CART ELITE
ASV Company	Trustwave Holdings, Inc.
Scan Compliance Status	Pass
Date Scan Completed	2017-10-28
Scan Expiration Date	2018-01-28



Part 2. Component Compliance Summary

#	Compliance Status	Name	Type	IP Address	Source	Critical	High	Medium	Low	Info
1	*Not In Scope*	www.shoppingcartelite.com	Web Site	104.25.86.104	Domain Name	0	0	12	0	21
					Total Findings	**0**	**0**	**12**	**0**	**21**
					Total PCI Vulnerabilities	**0**	**0**	**0**	**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	104.25.86.104 (www.shoppingcartelite.	Block cipher algorithms with block size of 64 bits (like DES and 3DES) birthday attack	Medium	5.00	Out of Scope	

#	IP Address	Vulnerabilities Noted	Severity	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
	com)	known as Sweet32, CVE-2016-2183				
2	104.25.86.104 (www.shoppingcartelite.com)	TLSv1.0 Supported	Medium	5.00	Out of Scope	**Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database. TLS v1.0 violates PCI DSS and is considered an automatic failing condition.
3	104.25.86.104 (www.shoppingcartelite.com)	Discovered HTTP Methods	Info	0.00	Out of Scope	
4	104.25.86.104 (www.shoppingcartelite.com)	Discovered Web Applications	Info	0.00	Out of Scope	
5	104.25.86.104 (www.shoppingcartelite.com)	Discovered Web Directories	Info	0.00	Out of Scope	
6	104.25.86.104 (www.shoppingcartelite.com)	Enumerated Applications	Info	0.00	Out of Scope	**Note to scan customer:** This vulnerability is not recognized in the National Vulnerability Database.
7	104.25.86.104 (www.shoppingcartelite.com)	Enumerated Hostnames	Info	0.00	Out of Scope	
8	104.25.86.104 (www.	Enumerated SSL/TLS Cipher Suites	Info	0.00	Out of Scope	

#	IP Address	Vulnerabilities Noted	Severity	CVSS Score	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
	shoppingcartelite.com)					
9	104.25.86.104 (www.shoppingcartelite.com)	Information Disclosure via robots.txt	Info	0.00	Out of Scope	
10	104.25.86.104 (www.shoppingcartelite.com)	SSLv2, SSLv3 and TLS v1.0 Vulnerable to CBC Attacks via chosen-plaintext (BEAST), CVE-2011-3389	Info	0.00	Out of Scope	**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:N/C:N/I:N/A:N, with a base score of 0.0.
11	104.25.86.104 (www.shoppingcartelite.com)	Unknown services found	Info	0.00	Out of Scope	

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.

Part 3b. Special Notes by IP Address

Vulnerability Scan Report: Executive Summary

#	IP Address	Note	Item Noted (remote access software, POS software, etc.)	Scan customer's declaration that software is implemented securely (see next column if not implemented securely)	Scan customer's description of actions taken to either: 1) remove the software or 2) implement security controls to secure the software
1	104.25.86.104 (www.shoppingcartelite.com)	**Unknown services** Note to scan customer: Unidentified services have been detected. Due to increased risk to the cardholder data environment, identify the service, then either 1) justify the business need for this service and confirm it is securely implemented, or 2) identify the service and confirm that it is disabled. Consult your ASV if you have questions about this Special Note.			

Vulnerability Scan Report: Vulnerability Details

Part 1. Scan Information

Scan Customer Company	SHOPPING CART ELITE	Date Scan Completed	2017-10-28
ASV Company	Trustwave Holdings, Inc.	Scan Expiration Date	2018-01-28

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	104.25.86.104 (www.shoppingcartelite.com)			true	tcp/80	http		cloudflare-nginx
					tcp/443	http		cloudflare-nginx
					tcp/2052	http		cloudflare-nginx
					tcp/2053	generic_ssl		

Vulnerability Scan Report: Vulnerability Details

#	Device	Names	OS	Ping	Service Information			
					Port	Protocol	Application	Detail
					tcp/2082	http		cloudflare-nginx
					tcp/2083	generic_ssl		
					tcp/2086	http		cloudflare-nginx
					tcp/2087	generic_ssl		
					tcp/2095	http		cloudflare-nginx
					tcp/2096	generic_ssl		
					tcp/8080	http		cloudflare-nginx
					tcp/8443	generic_ssl		
					tcp/8880	http		cloudflare-nginx
					All other scanned ports were filtered.			

Part 3a. Previous Scan Targets (Not Scanned)

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

#	Name	Type	IP Address	Date Removed
1	www.eccowarninglights.com	Web Site		2017-06-15

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	173.0.137.191	mail3.shoppingcartelite.net	Discovered hosts using second-level domain name(s): shoppingcartelite.com
2	173.245.58.141	rose.ns.cloudflare.com	Discovered hosts using second-level domain name(s): shoppingcartelite.com
3	173.245.59.118	ian.ns.cloudflare.com	Discovered hosts using second-level domain name(s): shoppingcartelite.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.

104.25.86.104 (www.shoppingcartelite.com)

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
1		TLSv1.0 Supported	5.00	Medium	Pass	**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:** http

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-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-

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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.
2	CVE-2016-2183	Block cipher algorithms with block size of 64 bits (like DES and 3DES) birthday attack known as Sweet32	5.00	Medium	Pass	**Port:** tcp/443 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. NOTE: Cipher block size must not be confused with key length. DES / 3DES ciphers are vulnerable because they always operate on 64 bit blocks regardless of the key length. If this vulnerability is detected, and in the list of detected ciphers you see only entries with numbers

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						different than 64 (eg. TLSv1 112 bits ECDHE-RSA-DES-CBC3-SHA), the detection is still valid, because '112 bits' is the key length. **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 : DES-CBC3-SHA **Remediation:** This issue can by avoided by disabling block ciphers of 64 bit block 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.

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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).
3		TLSv1.0 Supported	5.00	Medium	Pass	**Port:** tcp/2053 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:** generic_ssl **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/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-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

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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.
4	CVE-2016-2183	Block cipher algorithms with block size of 64 bits (like DES and 3DES) birthday attack known as Sweet32	5.00	Medium	Pass	**Port:** tcp/2053 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. NOTE: Cipher block size must not be confused with key length. DES / 3DES ciphers are vulnerable because they always operate on 64 bit blocks regardless of the key length. If this vulnerability is detected, and in the list of detected ciphers you see only entries with numbers different than 64 (eg. TLSv1 112 bits ECDHE-RSA-DES-CBC3-SHA), the detection is still valid, because '112 bits' is the key length. **CVE:** CVE-2016-2183 **NVD:** CVE-2016-2183 **CVSSv2:** AV:N/AC:L/Au:N/C:P/I:N/A:N **Service:** generic_ssl **Reference:** https://access.redhat.com/security/cve/cve-2016-2183

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						https://sweet32.info/ https://www.openssl.org/blog/blog/2016/08/24/sweet32/ **Evidence:** Cipher Suite: TLSv1 : DES-CBC3-SHA **Remediation:** This issue can by avoided by disabling block ciphers of 64 bit block 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

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
5		TLSv1.0 Supported	5.00	Medium	Pass	**Port:** tcp/2083 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:** generic_ssl **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 : AES256-SHA

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-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 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.
6	CVE-2016-2183	Block cipher algorithms with block size of 64 bits (like DES and 3DES)	5.00	Medium	Pass	**Port:** tcp/2083 This is a cipher vulnerability, not limited to any specific SSL/TLS software implementation. DES and Tripple DES (3DES) block ciphers

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
		birthday attack known as Sweet32				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. NOTE: Cipher block size must not be confused with key length. DES / 3DES ciphers are vulnerable because they always operate on 64 bit blocks regardless of the key length. If this vulnerability is detected, and in the list of detected ciphers you see only entries with numbers different than 64 (eg. TLSv1 112 bits ECDHE-RSA-DES-CBC3-SHA), the detection is still valid, because '112 bits' is the key length. **CVE:** CVE-2016-2183 **NVD:** CVE-2016-2183 **CVSSv2:** AV:N/AC:L/Au:N/C:P/I:N/A:N **Service:** generic_ssl **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 : DES-CBC3-SHA **Remediation:** This issue can by avoided by disabling block ciphers of 64 bit block 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).

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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).
7		TLSv1.0 Supported	5.00	Medium	Pass	**Port:** tcp/2087 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:** generic_ssl **Reference:**

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-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

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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.
8	CVE-2016-2183	Block cipher algorithms with block size of 64 bits (like DES and 3DES) birthday attack known as Sweet32	5.00	Medium	Pass	**Port:** tcp/2087 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. NOTE: Cipher block size must not be confused with key length. DES / 3DES ciphers are vulnerable because they always operate on 64 bit blocks regardless of the key length. If this vulnerability is detected, and in the list of detected ciphers you see only entries with numbers different than 64 (eg. TLSv1 112 bits ECDHE-RSA-DES-CBC3-SHA), the detection is still valid, because '112 bits' is the key length.

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						CVE: CVE-2016-2183 **NVD:** CVE-2016-2183 **CVSSv2:** AV:N/AC:L/Au:N/C:P/I:N/A:N **Service:** generic_ssl **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 : DES-CBC3-SHA **Remediation:** This issue can by avoided by disabling block ciphers of 64 bit block 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

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						'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).
9		TLSv1.0 Supported	5.00	Medium	Pass	**Port:** tcp/2096 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:** generic_ssl **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/

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-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

104.25.86.104 (www.shoppingcartelite.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.
10	CVE-2016-2183	Block cipher algorithms with block size of 64 bits (like DES and 3DES) birthday attack known as Sweet32	5.00	Medium	Pass	**Port:** tcp/2096 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. NOTE: Cipher block size must not be confused with key length. DES / 3DES ciphers are vulnerable because they always operate on 64 bit blocks regardless of the key length. If this vulnerability is detected, and in the list of detected ciphers you see only entries with numbers different than 64 (eg. TLSv1 112 bits ECDHE-RSA-DES-CBC3-SHA), the detection is still valid, because '112 bits' is the key length. **CVE:** CVE-2016-2183 **NVD:** CVE-2016-2183 **CVSSv2:** AV:N/AC:L/Au:N/C:P/I:N/A:N **Service:** generic_ssl **Reference:** https://access.redhat.com/security/cve/cve-2016-2183 https://sweet32.info/ https://www.openssl.org/blog/blog/2016/08/24/sweet32/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Evidence: Cipher Suite: TLSv1 : DES-CBC3-SHA **Remediation:** This issue can by avoided by disabling block ciphers of 64 bit block 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).
11		TLSv1.0 Supported	5.00	Medium	Pass	**Port:** tcp/8443

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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:** generic_ssl **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 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1 : AES128-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 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.
12	CVE-2016-2183	Block cipher algorithms with block size of 64 bits (like DES and 3DES) birthday attack known as	5.00	Medium	Pass	**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

104.25.86.104 (www.shoppingcartelite.com)

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
		Sweet32				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. NOTE: Cipher block size must not be confused with key length. DES / 3DES ciphers are vulnerable because they always operate on 64 bit blocks regardless of the key length. If this vulnerability is detected, and in the list of detected ciphers you see only entries with numbers different than 64 (eg. TLSv1 112 bits ECDHE-RSA-DES-CBC3-SHA), the detection is still valid, because '112 bits' is the key length. **CVE:** CVE-2016-2183 **NVD:** CVE-2016-2183 **CVSSv2:** AV:N/AC:L/Au:N/C:P/I:N/A:N **Service:** generic_ssl **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 : DES-CBC3-SHA **Remediation:** This issue can by avoided by disabling block ciphers of 64 bit block 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).

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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).
13	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.

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : DES-CBC3-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.
14		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

104.25.86.104 (www.shoppingcartelite.com)

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						and configuration of the remote SSL/TLS service. The information provided as part of this finding includes the SSL version (ex: TLSv1) as well as the name of the cipher suite (ex: RC4-SHA). A cipher suite is a set of cryptographic algorithms that provide authentication, encryption, and message authentication code (MAC) as part of an SSL/TLS negotiation and through the lifetime of the SSL session. It is typical that an SSL service would support multiple cipher suites. A cipher suite can be supported by across multiple SSL/TLS versions, so you should be of no concern to see the same cipher name reported for multiple **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Reference:** http://www.openssl.org/docs/apps/ciphers.html **Evidence:** Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : DES-CBC3-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : AES256-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : AES128-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : AES256-SHA256 Cipher Suite: TLSv1_2 : AES256-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA **Remediation:** No remediation is necessary.
15		Discovered Web Directories	0.00	Info	Pass	**Port:** tcp/443 It was possible to guess one or more directories contained in the publicly accessible path of this web server. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Evidence:** URL: https://104.25.86.104:443/statistics/ HTTP Response Code: 403

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/awstats-cgi/ URL: https://104.25.86.104:443/batavi/ URL: https://104.25.86.104:443/bitweaver/ URL: https://104.25.86.104:443/webalizer/ URL: https://104.25.86.104:443/login/ URL: https://104.25.86.104:443/_utils/ URL: https://104.25.86.104:443/cpcommerce/ URL: https://104.25.86.104:443/cubecart/ URL: https://104.25.86.104:443/pinnacle/ URL: https://104.25.86.104:443/kart/ URL: https://104.25.86.104:443/dotnetnuke/ URL: https://104.25.86.104:443/dnn/ URL: https://104.25.86.104:443/cms/ URL: https://104.25.86.104:443/drupal5/ URL: https://104.25.86.104:443/drupal6/ URL: https://104.25.86.104:443/drupal7/ URL: https://104.25.86.104:443/drupal/ URL: https://104.25.86.104:443/GScart/ URL: https://104.25.86.104:443/cart/ URL: https://104.25.86.104:443/productcart/ URL: https://104.25.86.104:443/pc/ URL: https://104.25.86.104:443/horde/ URL: https://104.25.86.104:443/webmail/ URL: https://104.25.86.104:443/horde-webmail/ URL: https://104.25.86.104:443/horde2/ URL: https://104.25.86.104:443/horde3/ URL: https://104.25.86.104:443/horde4/ URL: https://104.25.86.104:443/onecms/ URL: https://104.25.86.104:443/OneCMS/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/vsadmin/ URL: https://104.25.86.104:443/web-console/ URL: https://104.25.86.104:443/admin-console/ URL: https://104.25.86.104:443/jmx-console/ URL: https://104.25.86.104:443/jenkins/ URL: https://104.25.86.104:443/wp/ URL: https://104.25.86.104:443/wordpress/ URL: https://104.25.86.104:443/joomla/ URL: https://104.25.86.104:443/content/ URL: https://104.25.86.104:443/livecart/ URL: https://104.25.86.104:443/downloader/ URL: https://104.25.86.104:443/mambo/ URL: https://104.25.86.104:443/cms/typo3conf/ext/mk_anydropdownmenu/ URL: https://104.25.86.104:443/certsrv/ URL: https://104.25.86.104:443/SMSReporting_XYZ/ URL: https://104.25.86.104:443/ts/ URL: https://104.25.86.104:443/tfs/ URL: https://104.25.86.104:443/TFS/ URL: https://104.25.86.104:443/moodle/ URL: https://104.25.86.104:443/webcart/ URL: https://104.25.86.104:443/webcart11/ URL: https://104.25.86.104:443/webcart-lite/ URL: https://104.25.86.104:443/mt/ URL: https://104.25.86.104:443/mt-static/ URL: https://104.25.86.104:443/bugzilla/ URL: https://104.25.86.104:443/cgiwrap/ URL: https://104.25.86.104:443/servlet/ URL: https://104.25.86.104:443/opencart/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/opennms/ URL: https://104.25.86.104:443/em/ URL: https://104.25.86.104:443/console/ URL: https://104.25.86.104:443/oscommerce/ URL: https://104.25.86.104:443/phpfusion/ URL: https://104.25.86.104:443/php-fusion/ URL: https://104.25.86.104:443/phpBB3/ URL: https://104.25.86.104:443/phpBB/ URL: https://104.25.86.104:443/forum/ URL: https://104.25.86.104:443/phpcart/ URL: https://104.25.86.104:443/lists/ URL: https://104.25.86.104:443/phplist/ URL: https://104.25.86.104:443/phpMyAdmin/ URL: https://104.25.86.104:443/phpmyadmin/ URL: https://104.25.86.104:443/phproxy/ URL: https://104.25.86.104:443/phpslash-0.6/ URL: https://104.25.86.104:443/phpslash-0.61/ URL: https://104.25.86.104:443/phpslash-0.6.1/ URL: https://104.25.86.104:443/phpslash-0.6.2/ URL: https://104.25.86.104:443/phpslash-0.6.5/ URL: https://104.25.86.104:443/phpslash-065/ URL: https://104.25.86.104:443/phpslash-0.7.1/ URL: https://104.25.86.104:443/phpslash-0.7.2/ URL: https://104.25.86.104:443/phpslash-0.8/ URL: https://104.25.86.104:443/phpslash-0.8.1/ URL: https://104.25.86.104:443/phpslash/ URL: https://104.25.86.104:443/phpSlash/ URL: https://104.25.86.104:443/postfixadmin/ URL: https://104.25.86.104:443/projectpier/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/shellinabox/ URL: https://104.25.86.104:443/silverstripe/ URL: https://104.25.86.104:443/sit/ URL: https://104.25.86.104:443/smarty/ URL: https://104.25.86.104:443/squirrelmail/ URL: https://104.25.86.104:443/sm/ URL: https://104.25.86.104:443/sugarcrm/ URL: https://104.25.86.104:443/sugar/ URL: https://104.25.86.104:443/SugarCRM/ URL: https://104.25.86.104:443/sugarsuite/ URL: https://104.25.86.104:443/crm/ URL: https://104.25.86.104:443/textpattern/ URL: https://104.25.86.104:443/esp/ URL: https://104.25.86.104:443/forums/ URL: https://104.25.86.104:443/vb/ URL: https://104.25.86.104:443/en/ URL: https://104.25.86.104:443/vpasp/ URL: https://104.25.86.104:443/wavsep/ URL: https://104.25.86.104:443/wb/ URL: https://104.25.86.104:443/wb260/ URL: https://104.25.86.104:443/shop/ URL: https://104.25.86.104:443/zencart/ URL: https://104.25.86.104:443/zen-cart/ URL: https://104.25.86.104:443/zimbra/ URL: https://104.25.86.104:443/zimbraAdmin/ URL: https://104.25.86.104:443/.cobalt/ URL: https://104.25.86.104:443/_archive/ URL: https://104.25.86.104:443/_backup/ URL: https://104.25.86.104:443/_cti_pvt/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/_derived/ URL: https://104.25.86.104:443/_errors/ URL: https://104.25.86.104:443/_fpclass/ URL: https://104.25.86.104:443/_mem_bin/ URL: https://104.25.86.104:443/_notes/ URL: https://104.25.86.104:443/_objects/ URL: https://104.25.86.104:443/_old/ URL: https://104.25.86.104:443/_pages/ URL: https://104.25.86.104:443/_passwords/ URL: https://104.25.86.104:443/_private/ URL: https://104.25.86.104:443/_ScriptLibrary/ URL: https://104.25.86.104:443/_scripts/ URL: https://104.25.86.104:443/_sharedtemplates/ URL: https://104.25.86.104:443/_tests/ URL: https://104.25.86.104:443/_themes/ URL: https://104.25.86.104:443/_vti_bin/ URL: https://104.25.86.104:443/_vti_bot/ URL: https://104.25.86.104:443/_vti_log/ URL: https://104.25.86.104:443/_vti_pvt/ URL: https://104.25.86.104:443/_vti_shm/ URL: https://104.25.86.104:443/_vti_txt/ URL: https://104.25.86.104:443/~1/ URL: https://104.25.86.104:443/~admin/ URL: https://104.25.86.104:443/~log/ URL: https://104.25.86.104:443/~root/ URL: https://104.25.86.104:443/~stats/ URL: https://104.25.86.104:443/~webstats/ URL: https://104.25.86.104:443/about/ URL: https://104.25.86.104:443/access/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/accessplatform/ URL: https://104.25.86.104:443/accesswatch/ URL: https://104.25.86.104:443/account/ URL: https://104.25.86.104:443/accounting/ URL: https://104.25.86.104:443/acid/ URL: https://104.25.86.104:443/activex/ URL: https://104.25.86.104:443/adm/ URL: https://104.25.86.104:443/admcgi/ URL: https://104.25.86.104:443/admentor/ URL: https://104.25.86.104:443/Admin/ URL: https://104.25.86.104:443/admin.back/ URL: https://104.25.86.104:443/admin_/ URL: https://104.25.86.104:443/Admin_files/ URL: https://104.25.86.104:443/admin-bak/ URL: https://104.25.86.104:443/Administration/ URL: https://104.25.86.104:443/administrator/ URL: https://104.25.86.104:443/admin-old/ URL: https://104.25.86.104:443/adminuser/ URL: https://104.25.86.104:443/AdminWeb/ URL: https://104.25.86.104:443/admisapi/ URL: https://104.25.86.104:443/advwebadmin/ URL: https://104.25.86.104:443/Agent/ URL: https://104.25.86.104:443/Agents/ URL: https://104.25.86.104:443/Album/ URL: https://104.25.86.104:443/analog/ URL: https://104.25.86.104:443/anthill/ URL: https://104.25.86.104:443/apache/ URL: https://104.25.86.104:443/apex/ URL: https://104.25.86.104:443/app/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/applets/ URL: https://104.25.86.104:443/application/ URL: https://104.25.86.104:443/applications/ URL: https://104.25.86.104:443/applicattion/ URL: https://104.25.86.104:443/applicattions/ URL: https://104.25.86.104:443/apps/ URL: https://104.25.86.104:443/archive/ URL: https://104.25.86.104:443/archives/ URL: https://104.25.86.104:443/archivo/ URL: https://104.25.86.104:443/asdf/ URL: https://104.25.86.104:443/asp/ URL: https://104.25.86.104:443/aspx/ URL: https://104.25.86.104:443/atc/ URL: https://104.25.86.104:443/auth/ URL: https://104.25.86.104:443/authadmin/ URL: https://104.25.86.104:443/b2-include/ URL: https://104.25.86.104:443/back/ URL: https://104.25.86.104:443/backdoor/ URL: https://104.25.86.104:443/backend/ URL: https://104.25.86.104:443/backup/ URL: https://104.25.86.104:443/backups/ URL: https://104.25.86.104:443/bak/ URL: https://104.25.86.104:443/balancer/ URL: https://104.25.86.104:443/bank/ URL: https://104.25.86.104:443/banner/ URL: https://104.25.86.104:443/banner01/ URL: https://104.25.86.104:443/banners/ URL: https://104.25.86.104:443/basilix/ URL: https://104.25.86.104:443/batch/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/bb-dnbd/ URL: https://104.25.86.104:443/bbv/ URL: https://104.25.86.104:443/bdata/ URL: https://104.25.86.104:443/beta/ URL: https://104.25.86.104:443/billpay/ URL: https://104.25.86.104:443/bin/ URL: https://104.25.86.104:443/bmp/ URL: https://104.25.86.104:443/boadmin/ URL: https://104.25.86.104:443/boot/ URL: https://104.25.86.104:443/Boutiques/ URL: https://104.25.86.104:443/btauxdir/ URL: https://104.25.86.104:443/bug/ URL: https://104.25.86.104:443/bugs/ URL: https://104.25.86.104:443/business/ URL: https://104.25.86.104:443/buy/ URL: https://104.25.86.104:443/buynow/ URL: https://104.25.86.104:443/cache-stats/ URL: https://104.25.86.104:443/cacti/ URL: https://104.25.86.104:443/caja/ URL: https://104.25.86.104:443/card/ URL: https://104.25.86.104:443/cards/ URL: https://104.25.86.104:443/cash/ URL: https://104.25.86.104:443/catalog/ URL: https://104.25.86.104:443/cbi-bin/ URL: https://104.25.86.104:443/ccard/ URL: https://104.25.86.104:443/ccards/ URL: https://104.25.86.104:443/cd-cgi/ URL: https://104.25.86.104:443/cdrom/ URL: https://104.25.86.104:443/cert/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/certificate/ URL: https://104.25.86.104:443/cfdocs/ URL: https://104.25.86.104:443/CFIDE/ URL: https://104.25.86.104:443/cgi/ URL: https://104.25.86.104:443/cgi-auth/ URL: https://104.25.86.104:443/cgi-bim/ URL: https://104.25.86.104:443/cgibin/ URL: https://104.25.86.104:443/cgi-bin2/ URL: https://104.25.86.104:443/cgi-csc/ URL: https://104.25.86.104:443/cgi-isapi/ URL: https://104.25.86.104:443/cgilib/ URL: https://104.25.86.104:443/cgi-lib/ URL: https://104.25.86.104:443/cgi-local/ URL: https://104.25.86.104:443/cgis/ URL: https://104.25.86.104:443/cgiscripts/ URL: https://104.25.86.104:443/cgi-scripts/ URL: https://104.25.86.104:443/cgi-shl/ URL: https://104.25.86.104:443/cgi-shop/ URL: https://104.25.86.104:443/cgi-sys/ URL: https://104.25.86.104:443/cgi-weddico/ URL: https://104.25.86.104:443/cgiwin/ URL: https://104.25.86.104:443/cgi-win/ URL: https://104.25.86.104:443/chat/ URL: https://104.25.86.104:443/citrix/ URL: https://104.25.86.104:443/class/ URL: https://104.25.86.104:443/classes/ URL: https://104.25.86.104:443/client/ URL: https://104.25.86.104:443/cliente/ URL: https://104.25.86.104:443/clients/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/cobalt-images/ URL: https://104.25.86.104:443/code/ URL: https://104.25.86.104:443/com/ URL: https://104.25.86.104:443/comments/ URL: https://104.25.86.104:443/common/ URL: https://104.25.86.104:443/communicator/ URL: https://104.25.86.104:443/company/ URL: https://104.25.86.104:443/compressed/ URL: https://104.25.86.104:443/conf/ URL: https://104.25.86.104:443/config/ URL: https://104.25.86.104:443/connect/ URL: https://104.25.86.104:443/controlpanel/ URL: https://104.25.86.104:443/core/ URL: https://104.25.86.104:443/corp/ URL: https://104.25.86.104:443/Corporate/ URL: https://104.25.86.104:443/counter/ URL: https://104.25.86.104:443/cpanel/ URL: https://104.25.86.104:443/credit/ URL: https://104.25.86.104:443/cron/ URL: https://104.25.86.104:443/crons/ URL: https://104.25.86.104:443/crypto/ URL: https://104.25.86.104:443/csr/ URL: https://104.25.86.104:443/css/ URL: https://104.25.86.104:443/currency/ URL: https://104.25.86.104:443/custdata/ URL: https://104.25.86.104:443/customers/ URL: https://104.25.86.104:443/CVS/ URL: https://104.25.86.104:443/cvsweb/ URL: https://104.25.86.104:443/cybercash/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/darkportal/ URL: https://104.25.86.104:443/dat/ URL: https://104.25.86.104:443/data/ URL: https://104.25.86.104:443/database/ URL: https://104.25.86.104:443/databases/ URL: https://104.25.86.104:443/datafiles/ URL: https://104.25.86.104:443/dato/ URL: https://104.25.86.104:443/datos/ URL: https://104.25.86.104:443/db/ URL: https://104.25.86.104:443/DB4Web/ URL: https://104.25.86.104:443/dbase/ URL: https://104.25.86.104:443/dcforum/ URL: https://104.25.86.104:443/ddreport/ URL: https://104.25.86.104:443/ddrint/ URL: https://104.25.86.104:443/demo/ URL: https://104.25.86.104:443/demomall/ URL: https://104.25.86.104:443/demos/ URL: https://104.25.86.104:443/design/ URL: https://104.25.86.104:443/dev/ URL: https://104.25.86.104:443/devel/ URL: https://104.25.86.104:443/development/ URL: https://104.25.86.104:443/dir/ URL: https://104.25.86.104:443/directory/ URL: https://104.25.86.104:443/directorymanager/ URL: https://104.25.86.104:443/dl/ URL: https://104.25.86.104:443/dll/ URL: https://104.25.86.104:443/dm/ URL: https://104.25.86.104:443/DMR/ URL: https://104.25.86.104:443/dms/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/dms0/ URL: https://104.25.86.104:443/dmsdump/ URL: https://104.25.86.104:443/doc/ URL: https://104.25.86.104:443/doc1/ URL: https://104.25.86.104:443/doc-html/ URL: https://104.25.86.104:443/docs/ URL: https://104.25.86.104:443/docs1/ URL: https://104.25.86.104:443/DocuColor/ URL: https://104.25.86.104:443/document/ URL: https://104.25.86.104:443/documents/ URL: https://104.25.86.104:443/down/ URL: https://104.25.86.104:443/download/ URL: https://104.25.86.104:443/downloads/ URL: https://104.25.86.104:443/dump/ URL: https://104.25.86.104:443/durep/ URL: https://104.25.86.104:443/dynamic/ URL: https://104.25.86.104:443/easylog/ URL: https://104.25.86.104:443/eforum/ URL: https://104.25.86.104:443/email/ URL: https://104.25.86.104:443/emailclass/ URL: https://104.25.86.104:443/eManager/ URL: https://104.25.86.104:443/employees/ URL: https://104.25.86.104:443/empoyees/ URL: https://104.25.86.104:443/empris/ URL: https://104.25.86.104:443/en-US/ URL: https://104.25.86.104:443/error/ URL: https://104.25.86.104:443/errors/ URL: https://104.25.86.104:443/es/ URL: https://104.25.86.104:443/estmt/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/etc/ URL: https://104.25.86.104:443/example/ URL: https://104.25.86.104:443/examples/ URL: https://104.25.86.104:443/exchange/ URL: https://104.25.86.104:443/EXE/ URL: https://104.25.86.104:443/exec/ URL: https://104.25.86.104:443/export/ URL: https://104.25.86.104:443/external/ URL: https://104.25.86.104:443/faq/ URL: https://104.25.86.104:443/fcgi-bin/ URL: https://104.25.86.104:443/fileadmin/ URL: https://104.25.86.104:443/filemanager/ URL: https://104.25.86.104:443/files/ URL: https://104.25.86.104:443/foldoc/ URL: https://104.25.86.104:443/form/ URL: https://104.25.86.104:443/forms/ URL: https://104.25.86.104:443/formsmgr/ URL: https://104.25.86.104:443/fpadmin/ URL: https://104.25.86.104:443/fpdb/ URL: https://104.25.86.104:443/fpsample/ URL: https://104.25.86.104:443/fr/ URL: https://104.25.86.104:443/frameset/ URL: https://104.25.86.104:443/framesets/ URL: https://104.25.86.104:443/ftp/ URL: https://104.25.86.104:443/ftproot/ URL: https://104.25.86.104:443/global/ URL: https://104.25.86.104:443/graphics/ URL: https://104.25.86.104:443/guest/ URL: https://104.25.86.104:443/guestbook/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/guests/ URL: https://104.25.86.104:443/help/ URL: https://104.25.86.104:443/helpdesk/ URL: https://104.25.86.104:443/hidden/ URL: https://104.25.86.104:443/hide/ URL: https://104.25.86.104:443/hit_tracker/ URL: https://104.25.86.104:443/hitmatic/ URL: https://104.25.86.104:443/hlstats/ URL: https://104.25.86.104:443/home/ URL: https://104.25.86.104:443/homepage/ URL: https://104.25.86.104:443/howto/ URL: https://104.25.86.104:443/hp_docs/ URL: https://104.25.86.104:443/hp-ux/ URL: https://104.25.86.104:443/htbin/ URL: https://104.25.86.104:443/htdocs/ URL: https://104.25.86.104:443/hyperstat/ URL: https://104.25.86.104:443/ibank/ URL: https://104.25.86.104:443/ibill/ URL: https://104.25.86.104:443/IBMWebAS/ URL: https://104.25.86.104:443/icons/ URL: https://104.25.86.104:443/idea/ URL: https://104.25.86.104:443/ideas/ URL: https://104.25.86.104:443/iisadmin/ URL: https://104.25.86.104:443/iisprotect/ URL: https://104.25.86.104:443/iissamples/ URL: https://104.25.86.104:443/image/ URL: https://104.25.86.104:443/imagenes/ URL: https://104.25.86.104:443/imagery/ URL: https://104.25.86.104:443/images/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/img/ URL: https://104.25.86.104:443/imgs/ URL: https://104.25.86.104:443/img-sys/ URL: https://104.25.86.104:443/imp/ URL: https://104.25.86.104:443/import/ URL: https://104.25.86.104:443/inc/ URL: https://104.25.86.104:443/include/ URL: https://104.25.86.104:443/includes/ URL: https://104.25.86.104:443/incoming/ URL: https://104.25.86.104:443/info/ URL: https://104.25.86.104:443/information/ URL: https://104.25.86.104:443/install/ URL: https://104.25.86.104:443/interchange/ URL: https://104.25.86.104:443/internal/ URL: https://104.25.86.104:443/interscan/ URL: https://104.25.86.104:443/intl/ URL: https://104.25.86.104:443/intranet/ URL: https://104.25.86.104:443/inventory/ URL: https://104.25.86.104:443/isapi/ URL: https://104.25.86.104:443/j2ee/ URL: https://104.25.86.104:443/java/ URL: https://104.25.86.104:443/javadoc/ URL: https://104.25.86.104:443/java-plugin/ URL: https://104.25.86.104:443/javascript/ URL: https://104.25.86.104:443/javasdk/ URL: https://104.25.86.104:443/java-sys/ URL: https://104.25.86.104:443/javatest/ URL: https://104.25.86.104:443/javax/ URL: https://104.25.86.104:443/jdbc/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/jigsaw/ URL: https://104.25.86.104:443/job/ URL: https://104.25.86.104:443/jrun/ URL: https://104.25.86.104:443/js/ URL: https://104.25.86.104:443/jserv/ URL: https://104.25.86.104:443/jservdocs/ URL: https://104.25.86.104:443/jslib/ URL: https://104.25.86.104:443/jsp/ URL: https://104.25.86.104:443/jspdocs/ URL: https://104.25.86.104:443/jsp-examples/ URL: https://104.25.86.104:443/junk/ URL: https://104.25.86.104:443/kboard/ URL: https://104.25.86.104:443/keyserver/ URL: https://104.25.86.104:443/kiva/ URL: https://104.25.86.104:443/krysalis/ URL: https://104.25.86.104:443/labs/ URL: https://104.25.86.104:443/lampp/ URL: https://104.25.86.104:443/legal/ URL: https://104.25.86.104:443/lib/ URL: https://104.25.86.104:443/libraries/ URL: https://104.25.86.104:443/library/ URL: https://104.25.86.104:443/links/ URL: https://104.25.86.104:443/linux/ URL: https://104.25.86.104:443/livehelp/ URL: https://104.25.86.104:443/loader/ URL: https://104.25.86.104:443/log/ URL: https://104.25.86.104:443/logfile/ URL: https://104.25.86.104:443/logfiles/ URL: https://104.25.86.104:443/logger/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/logging/ URL: https://104.25.86.104:443/logon/ URL: https://104.25.86.104:443/logs/ URL: https://104.25.86.104:443/lost+found/ URL: https://104.25.86.104:443/mail/ URL: https://104.25.86.104:443/mail_log_files/ URL: https://104.25.86.104:443/mailman/ URL: https://104.25.86.104:443/mailroot/ URL: https://104.25.86.104:443/Main/ URL: https://104.25.86.104:443/makefile/ URL: https://104.25.86.104:443/manage/ URL: https://104.25.86.104:443/manual/ URL: https://104.25.86.104:443/market/ URL: https://104.25.86.104:443/marketing/ URL: https://104.25.86.104:443/member/ URL: https://104.25.86.104:443/members/ URL: https://104.25.86.104:443/message/ URL: https://104.25.86.104:443/messaging/ URL: https://104.25.86.104:443/MessagingManager/ URL: https://104.25.86.104:443/metacart/ URL: https://104.25.86.104:443/metaframe/ URL: https://104.25.86.104:443/misc/ URL: https://104.25.86.104:443/mkstats/ URL: https://104.25.86.104:443/msql/ URL: https://104.25.86.104:443/msword/ URL: https://104.25.86.104:443/myaccount/ URL: https://104.25.86.104:443/mysql/ URL: https://104.25.86.104:443/mysql_admin/ URL: https://104.25.86.104:443/na_admin/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/ncadmin/ URL: https://104.25.86.104:443/nchelp/ URL: https://104.25.86.104:443/ncsample/ URL: https://104.25.86.104:443/netbasic/ URL: https://104.25.86.104:443/netcat/ URL: https://104.25.86.104:443/NetDynamic/ URL: https://104.25.86.104:443/NetDynamics/ URL: https://104.25.86.104:443/nethome/ URL: https://104.25.86.104:443/netmagstats/ URL: https://104.25.86.104:443/netscape/ URL: https://104.25.86.104:443/netshare/ URL: https://104.25.86.104:443/nettracker/ URL: https://104.25.86.104:443/new/ URL: https://104.25.86.104:443/News/ URL: https://104.25.86.104:443/OA_HTML/ URL: https://104.25.86.104:443/OA_JAVA/ URL: https://104.25.86.104:443/OA_MEDIA/ URL: https://104.25.86.104:443/obj/ URL: https://104.25.86.104:443/objects/ URL: https://104.25.86.104:443/odbc/ URL: https://104.25.86.104:443/offers/ URL: https://104.25.86.104:443/old/ URL: https://104.25.86.104:443/old_files/ URL: https://104.25.86.104:443/oldfiles/ URL: https://104.25.86.104:443/oprocmgr-service/ URL: https://104.25.86.104:443/oprocmgr-status/ URL: https://104.25.86.104:443/oracle/ URL: https://104.25.86.104:443/oradata/ URL: https://104.25.86.104:443/order/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/orders/ URL: https://104.25.86.104:443/outgoing/ URL: https://104.25.86.104:443/owners/ URL: https://104.25.86.104:443/ows/ URL: https://104.25.86.104:443/pages/ URL: https://104.25.86.104:443/passport/ URL: https://104.25.86.104:443/password/ URL: https://104.25.86.104:443/passwords/ URL: https://104.25.86.104:443/payment/ URL: https://104.25.86.104:443/payments/ URL: https://104.25.86.104:443/pdf/ URL: https://104.25.86.104:443/pdfs/ URL: https://104.25.86.104:443/PDG_Cart/ URL: https://104.25.86.104:443/perl/ URL: https://104.25.86.104:443/perl5/ URL: https://104.25.86.104:443/personal/ URL: https://104.25.86.104:443/pforum/ URL: https://104.25.86.104:443/phorum/ URL: https://104.25.86.104:443/photo/ URL: https://104.25.86.104:443/php/ URL: https://104.25.86.104:443/php_classes/ URL: https://104.25.86.104:443/phpclassifieds/ URL: https://104.25.86.104:443/phpimageview/ URL: https://104.25.86.104:443/phpnuke/ URL: https://104.25.86.104:443/phpPhotoAlbum/ URL: https://104.25.86.104:443/phpprojekt/ URL: https://104.25.86.104:443/phpSecurePages/ URL: https://104.25.86.104:443/pics/ URL: https://104.25.86.104:443/piranha/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/pix/ URL: https://104.25.86.104:443/pls/ URL: https://104.25.86.104:443/po/ URL: https://104.25.86.104:443/postgres/ URL: https://104.25.86.104:443/ppwb/ URL: https://104.25.86.104:443/printers/ URL: https://104.25.86.104:443/priv/ URL: https://104.25.86.104:443/private/ URL: https://104.25.86.104:443/Program%20Files/ URL: https://104.25.86.104:443/protected/ URL: https://104.25.86.104:443/prv/ URL: https://104.25.86.104:443/pub/ URL: https://104.25.86.104:443/public/ URL: https://104.25.86.104:443/publish/ URL: https://104.25.86.104:443/publisher/ URL: https://104.25.86.104:443/purchase/ URL: https://104.25.86.104:443/pw/ URL: https://104.25.86.104:443/python/ URL: https://104.25.86.104:443/README/ URL: https://104.25.86.104:443/register/ URL: https://104.25.86.104:443/registered/ URL: https://104.25.86.104:443/Remote/ URL: https://104.25.86.104:443/report/ URL: https://104.25.86.104:443/reports/ URL: https://104.25.86.104:443/reseller/ URL: https://104.25.86.104:443/restricted/ URL: https://104.25.86.104:443/retail/ URL: https://104.25.86.104:443/reviews/ URL: https://104.25.86.104:443/root/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/sales/ URL: https://104.25.86.104:443/sample/ URL: https://104.25.86.104:443/script/ URL: https://104.25.86.104:443/scripts/ URL: https://104.25.86.104:443/search/ URL: https://104.25.86.104:443/search-ui/ URL: https://104.25.86.104:443/secret/ URL: https://104.25.86.104:443/secure/ URL: https://104.25.86.104:443/securecontrolpanel/ URL: https://104.25.86.104:443/secured/ URL: https://104.25.86.104:443/serve/ URL: https://104.25.86.104:443/server/ URL: https://104.25.86.104:443/server_stats/ URL: https://104.25.86.104:443/server-info/ URL: https://104.25.86.104:443/servers/ URL: https://104.25.86.104:443/serverstats/ URL: https://104.25.86.104:443/service/ URL: https://104.25.86.104:443/services/ URL: https://104.25.86.104:443/servlets/ URL: https://104.25.86.104:443/session/ URL: https://104.25.86.104:443/setup/ URL: https://104.25.86.104:443/share/ URL: https://104.25.86.104:443/shared/ URL: https://104.25.86.104:443/shell-cgi/ URL: https://104.25.86.104:443/shipping/ URL: https://104.25.86.104:443/shopper/ URL: https://104.25.86.104:443/shopping/ URL: https://104.25.86.104:443/SilverStream/ URL: https://104.25.86.104:443/site/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/siteadmin/ URL: https://104.25.86.104:443/sitebuildercontent/ URL: https://104.25.86.104:443/sitebuilderfiles/ URL: https://104.25.86.104:443/sitebuilderpictures/ URL: https://104.25.86.104:443/sitemgr/ URL: https://104.25.86.104:443/siteminder/ URL: https://104.25.86.104:443/siteminderagent/ URL: https://104.25.86.104:443/sites/ URL: https://104.25.86.104:443/siteseed/ URL: https://104.25.86.104:443/siteserver/ URL: https://104.25.86.104:443/sitestats/ URL: https://104.25.86.104:443/siteupdate/ URL: https://104.25.86.104:443/slide/ URL: https://104.25.86.104:443/smreports/ URL: https://104.25.86.104:443/smreportsviewer/ URL: https://104.25.86.104:443/soap/ URL: https://104.25.86.104:443/soapdocs/ URL: https://104.25.86.104:443/software/ URL: https://104.25.86.104:443/solaris/ URL: https://104.25.86.104:443/solutions/ URL: https://104.25.86.104:443/source/ URL: https://104.25.86.104:443/Sources/ URL: https://104.25.86.104:443/sql/ URL: https://104.25.86.104:443/squid/ URL: https://104.25.86.104:443/src/ URL: https://104.25.86.104:443/srchadm/ URL: https://104.25.86.104:443/ssdefs/ URL: https://104.25.86.104:443/sshome/ URL: https://104.25.86.104:443/ssi/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/ssl/ URL: https://104.25.86.104:443/sslkeys/ URL: https://104.25.86.104:443/staff/ URL: https://104.25.86.104:443/staging/ URL: https://104.25.86.104:443/stat/ URL: https://104.25.86.104:443/static/ URL: https://104.25.86.104:443/statistic/ URL: https://104.25.86.104:443/Statistics/ URL: https://104.25.86.104:443/stats_old/ URL: https://104.25.86.104:443/stats-bin-p/ URL: https://104.25.86.104:443/storage/ URL: https://104.25.86.104:443/StoreDB/ URL: https://104.25.86.104:443/storemgr/ URL: https://104.25.86.104:443/stuff/ URL: https://104.25.86.104:443/style/ URL: https://104.25.86.104:443/styles/ URL: https://104.25.86.104:443/stylesheet/ URL: https://104.25.86.104:443/stylesheets/ URL: https://104.25.86.104:443/subir/ URL: https://104.25.86.104:443/sun/ URL: https://104.25.86.104:443/support/ URL: https://104.25.86.104:443/sys/ URL: https://104.25.86.104:443/sysadmin/ URL: https://104.25.86.104:443/sysbackup/ URL: https://104.25.86.104:443/system/ URL: https://104.25.86.104:443/tar/ URL: https://104.25.86.104:443/tdbin/ URL: https://104.25.86.104:443/tech/ URL: https://104.25.86.104:443/technote/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/temp/ URL: https://104.25.86.104:443/template/ URL: https://104.25.86.104:443/test/ URL: https://104.25.86.104:443/test-cgi/ URL: https://104.25.86.104:443/testing/ URL: https://104.25.86.104:443/tests/ URL: https://104.25.86.104:443/testweb/ URL: https://104.25.86.104:443/themes/ URL: https://104.25.86.104:443/ticket/ URL: https://104.25.86.104:443/tickets/ URL: https://104.25.86.104:443/tiki/ URL: https://104.25.86.104:443/tmp/ URL: https://104.25.86.104:443/tools/ URL: https://104.25.86.104:443/track/ URL: https://104.25.86.104:443/tracking/ URL: https://104.25.86.104:443/trafficlog/ URL: https://104.25.86.104:443/updates/ URL: https://104.25.86.104:443/upload/ URL: https://104.25.86.104:443/uploads/ URL: https://104.25.86.104:443/us/ URL: https://104.25.86.104:443/usage/ URL: https://104.25.86.104:443/user/ URL: https://104.25.86.104:443/userdb/ URL: https://104.25.86.104:443/users/ URL: https://104.25.86.104:443/usr/ URL: https://104.25.86.104:443/ustats/ URL: https://104.25.86.104:443/util/ URL: https://104.25.86.104:443/utils/ URL: https://104.25.86.104:443/w3c/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/web/ URL: https://104.25.86.104:443/Web_store/ URL: https://104.25.86.104:443/web_usage/ URL: https://104.25.86.104:443/webaccess/ URL: https://104.25.86.104:443/webadmin/ URL: https://104.25.86.104:443/webapps/ URL: https://104.25.86.104:443/WebBank/ URL: https://104.25.86.104:443/webboard/ URL: https://104.25.86.104:443/webcache/ URL: https://104.25.86.104:443/WebCalendar/ URL: https://104.25.86.104:443/webcgi/ URL: https://104.25.86.104:443/webdata/ URL: https://104.25.86.104:443/webdav/ URL: https://104.25.86.104:443/WebDB/ URL: https://104.25.86.104:443/webimages/ URL: https://104.25.86.104:443/webimages2/ URL: https://104.25.86.104:443/weblog/ URL: https://104.25.86.104:443/weblogs/ URL: https://104.25.86.104:443/webmaster/ URL: https://104.25.86.104:443/webmaster_logs/ URL: https://104.25.86.104:443/webpub/ URL: https://104.25.86.104:443/webpub-ui/ URL: https://104.25.86.104:443/webreports/ URL: https://104.25.86.104:443/webshare/ URL: https://104.25.86.104:443/WebShop/ URL: https://104.25.86.104:443/website/ URL: https://104.25.86.104:443/webstat/ URL: https://104.25.86.104:443/webstats/ URL: https://104.25.86.104:443/webtrace/

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://104.25.86.104:443/WebTrend/ URL: https://104.25.86.104:443/webtrends/ URL: https://104.25.86.104:443/windows/ URL: https://104.25.86.104:443/WSsamples/ URL: https://104.25.86.104:443/wstats/ URL: https://104.25.86.104:443/www/ URL: https://104.25.86.104:443/www-sql/ URL: https://104.25.86.104:443/wwwstat/ URL: https://104.25.86.104:443/wwwstats/ URL: https://104.25.86.104:443/xenapp/ URL: https://104.25.86.104:443/xml/ URL: https://104.25.86.104:443/XSL/ URL: https://104.25.86.104:443/zipfiles/ **Remediation:** Review these directories and verify that there is no unintentional content made available to remote users.
16		Enumerated Applications	0.00	Info	Pass	**Port:** tcp/443 The following applications have been enumerated on this device. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Evidence:** CPE: microsoft:.net_framework URI: / Version: unknown

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Remediation: No remediation is required.
17		Enumerated Applications	0.00	Info	Pass	**Port:** tcp/443 The following applications have been enumerated on this device. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Evidence:** CPE: microsoft:asp.net URI: / Version: 4.0.30319 **Remediation:** No remediation is required.
18		Information Disclosure via robots.txt	0.00	Info	Pass	**Port:** tcp/443 Some Web Servers use a file called /robot(s).txt to make search engines and any other indexing tools visit their WebPages more frequently and more efficiently. By connecting to the server and requesting the /robot(s).txt file, an attacker may gain additional information about the system they are attacking. Such information as, restricted directories, hidden directories, cgi script directories and etc. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Service: http **Evidence:** URL: https://www.shoppingcartelite.com:443/robots.txt Rule found: Disallow: Rule found: Disallow: /Admin/ Rule found: Disallow: /App_Browser/ **Remediation:** Take special care not to tell the robots not to index sensitive directories, since this tells attackers exactly which of your directories are sensitive.
19		Discovered HTTP Methods	0.00	Info	Pass	**Port:** tcp/443 Requesting the allowed HTTP OPTIONS from this host shows which HTTP protocol methods are supported by its web server. Note that, in some cases, this information is not reported by the web server accurately. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Evidence:** URL: https://www.shoppingcartelite.com/ Methods: OPTIONS, TRACE, GET, HEAD, POST **Remediation:** Review your web server configuration and ensure that only those HTTP methods required for your business operations are enabled.

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
20		Discovered Web Applications	0.00	Info	Pass	**Port:** tcp/443 The following web applications were discovered on the remote HTTP server. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Remediation:** No remediation is required.
21		Discovered Web Directories	0.00	Info	Pass	**Port:** tcp/443 It was possible to guess one or more directories contained in the publicly accessible path of this web server. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** http **Evidence:** URL: https://www.shoppingcartelite.com:443/admin/ HTTP Response Code: 403 URL: https://www.shoppingcartelite.com:443/about/ HTTP Response Code: 410 URL: https://www.shoppingcartelite.com:443/Admin/ URL: https://www.shoppingcartelite.com:443/config/ URL: https://www.shoppingcartelite.com:443/faq/ URL: https://www.shoppingcartelite.com:443/images/

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						URL: https://www.shoppingcartelite.com:443/install/ URL: https://www.shoppingcartelite.com:443/js/ URL: https://www.shoppingcartelite.com:443/links/ URL: https://www.shoppingcartelite.com:443/scripts/ URL: https://www.shoppingcartelite.com:443/secured/ URL: https://www.shoppingcartelite.com:443/support/ HTTP Response Code: 301 **Remediation:** Review these directories and verify that there is no unintentional content made available to remote users.
22	CVE-2011-3389	SSLv2, SSLv3 and TLS v1.0 Vulnerable to CBC Attacks via chosen-plaintext (BEAST)	0.00	Info	Pass	**Port:** tcp/2053 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:** generic_ssl

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : DES-CBC3-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.
23		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	**Port:** tcp/2053 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

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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:** generic_ssl **Reference:** http://www.openssl.org/docs/apps/ciphers.html **Evidence:** Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : DES-CBC3-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : AES256-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : AES128-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : AES256-SHA256

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1_2 : AES256-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA **Remediation:** No remediation is necessary.
24	CVE-2011-3389	SSLv2, SSLv3 and TLS v1.0 Vulnerable to CBC Attacks via chosen-plaintext (BEAST)	0.00	Info	Pass	**Port:** tcp/2083 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:** generic_ssl

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : DES-CBC3-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.
25		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	**Port:** tcp/2083 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).

104.25.86.104 (www.shoppingcartelite.com)

#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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:** generic_ssl **Reference:** http://www.openssl.org/docs/apps/ciphers.html **Evidence:** Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : DES-CBC3-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : AES256-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : AES128-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : AES256-GCM-SHA384

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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-ECDSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA **Remediation:** No remediation is necessary.
26	CVE-2011-3389	SSLv2, SSLv3 and TLS v1.0 Vulnerable to CBC Attacks via chosen-plaintext (BEAST)	0.00	Info	Pass	**Port:** tcp/2087 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

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Service: generic_ssl **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 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : DES-CBC3-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.
27		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	**Port:** tcp/2087 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).

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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:** generic_ssl **Reference:** http://www.openssl.org/docs/apps/ciphers.html **Evidence:** Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : DES-CBC3-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : AES256-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : AES128-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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-ECDSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA **Remediation:** No remediation is necessary.
28	CVE-2011-3389	SSLv2, SSLv3 and TLS v1.0 Vulnerable to CBC Attacks via chosen-plaintext (BEAST)	0.00	Info	Pass	**Port:** tcp/2096 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

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						CVSSv2: AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** generic_ssl **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 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : DES-CBC3-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.
29		Enumerated SSL/TLS Cipher Suites	0.00	Info	Pass	**Port:** tcp/2096 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

104.25.86.104 (www.shoppingcartelite.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:** generic_ssl **Reference:** http://www.openssl.org/docs/apps/ciphers.html **Evidence:** Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : DES-CBC3-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : AES256-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : AES128-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : AES256-SHA256 Cipher Suite: TLSv1_2 : AES256-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA **Remediation:** No remediation is necessary.
30	CVE-2011-3389	SSLv2, SSLv3 and TLS v1.0 Vulnerable to CBC Attacks via chosen-plaintext (BEAST)	0.00	Info	Pass	**Port:** tcp/8443 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

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						NVD: CVE-2011-3389 **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Service:** generic_ssl **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 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : DES-CBC3-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.
31		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.

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						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:** generic_ssl **Reference:** http://www.openssl.org/docs/apps/ciphers.html **Evidence:** Cipher Suite: TLSv1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1 : AES256-SHA Cipher Suite: TLSv1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1 : AES128-SHA Cipher Suite: TLSv1 : DES-CBC3-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_1 : AES256-SHA Cipher Suite: TLSv1_1 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_1 : AES128-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA384

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES256-SHA384 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES256-SHA Cipher Suite: TLSv1_2 : AES256-GCM-SHA384 Cipher Suite: TLSv1_2 : AES256-SHA256 Cipher Suite: TLSv1_2 : AES256-SHA Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-ECDSA-AES128-SHA256 Cipher Suite: TLSv1_2 : ECDHE-RSA-AES128-SHA Cipher Suite: TLSv1_2 : AES128-GCM-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA256 Cipher Suite: TLSv1_2 : AES128-SHA **Remediation:** No remediation is necessary.
32		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: ssl370934.cloudflaressl.com, Source: SSL Certificate Subject Common Name Hostname: ssl370934.cloudflaressl.com, Source: SSL Certificate Subject subjectAltName DNS Hostname: am1380theanswer.com, Source: SSL Certificate Subject subjectAltName DNS Hostname: am870theanswer.com, Source: SSL Certificate Subject subjectAltName DNS

Vulnerability Scan Report: Vulnerability Details

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						Hostname: am920theanswer.com, Source: SSL Certificate Subject subjectAltName DNS Hostname: bachpan.com, Source: SSL Certificate Subject subjectAltName DNS Hostname: coalage.com, Source: SSL Certificate Subject subjectAltName DNS Hostname: connectedpictures.com, Source: SSL Certificate Subject subjectAltName DNS Hostname: geotimes.co.id, Source: SSL Certificate Subject subjectAltName DNS Hostname: manticus.at, Source: SSL Certificate Subject subjectAltName DNS Hostname: meltingsoft.com, Source: SSL Certificate Subject subjectAltName DNS Hostname: pc365.co.il, Source: SSL Certificate Subject subjectAltName DNS Hostname: scwsecurity.com, Source: SSL Certificate Subject subjectAltName DNS Hostname: security-camera-warehouse.com, Source: SSL Certificate Subject subjectAltName DNS Hostname: shoppingcartelite.com, Source: SSL Certificate Subject subjectAltName DNS Hostname: usefuloutdoortools.com, Source: SSL Certificate Subject subjectAltName DNS **Remediation:** No action is required.
33		Unknown services found	0.00	Info	Pass	The finding reports all ports and protocols that couldn't be remotely identified. Particular items may indicate uncommon but safe protocols or in-house application that uses custom and/or proprietary protocol.

104.25.86.104 (www.shoppingcartelite.com)						
#	CVE Number	Vulnerability	CVSS Score	Severity	Compliance Status	Details
						However they can as well indicate malicious activity (backdoors, rootkits, any other types of malware). This finding is purely informational. **CVSSv2:** AV:N/AC:L/Au:N/C:N/I:N/A:N **Evidence:** Unknown Service: transport protocol: tcp, port: 2053, ssl: true, banner: (N/A) Unknown Service: transport protocol: tcp, port: 2083, ssl: true, banner: (N/A) Unknown Service: transport protocol: tcp, port: 2087, ssl: true, banner: (N/A) Unknown Service: transport protocol: tcp, port: 2096, ssl: true, banner: (N/A) Unknown Service: transport protocol: tcp, port: 8443, ssl: true, banner: (N/A) **Remediation:** Review items mentioned in this finding one by one and ensure the services are known and accounted for in your security plan.

Vulnerability Scan Report: Vulnerability Details

Part 5a. Web Servers

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

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

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

#	System IP Address	Domain Name	Port	Server Type	Default Status and Title/Redirect
1	104.25.86.104 (www.shoppingcartelite.com)		tcp / 80		403 Forbidden - Direct IP access not allowed | Cloudflare
2	104.25.86.104 (www.shoppingcartelite.com)		tcp / 443		403 Forbidden - 403 Forbidden
3	104.25.86.104 (www.shoppingcartelite.com)		tcp / 2052		403 Forbidden - Direct IP access not allowed | Cloudflare
4	104.25.86.104 (www.shoppingcartelite.com)		tcp / 2082		403 Forbidden - Direct IP access not allowed | Cloudflare

#	System IP Address	Domain Name	Port	Server Type	Default Status and Title/Redirect
5	104.25.86.104 (www.shoppingcartelite.com)		tcp / 2086		403 Forbidden - Direct IP access not allowed | Cloudflare
6	104.25.86.104 (www.shoppingcartelite.com)		tcp / 2095		403 Forbidden - Direct IP access not allowed | Cloudflare
7	104.25.86.104 (www.shoppingcartelite.com)		tcp / 8080		403 Forbidden - Direct IP access not allowed | Cloudflare
8	104.25.86.104 (www.shoppingcartelite.com)		tcp / 8880		403 Forbidden - Direct IP access not allowed | Cloudflare

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
No SSL certificate information was discovered during the scan.				

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:	