

securityMETRICS®

# **ASV Scan Report Vulnerability Details**

**SIGMAALPHAEPSILON**

# Scan Results Table of Contents

Domain/IP	Max Risk	Domain/IP	Max Risk
<a href="http://63.128.2.12">63.128.2.12 (www.sae.net)</a>	<b>3</b>	<a href="http://12.200.135.2">12.200.135.2 (saevpn.sae.net)</a>	<b>2</b>
<a href="http://12.200.135.1">12.200.135.1</a>	<b>2</b>		

---

# Test Results

Executive Summary		
Test Result: <b>Pass</b>	Date: <b>2011-10-28</b>	Target IP: <b>63.128.2.12</b>
Test ID: <b>3283533</b>	Test Length: <b>2.70 Hours</b>	DNS Entry: <b>www.sae.net</b>
Total Risk: <b>9</b>	Start Time: <b>03:41:28</b>	Finish Time: <b>06:23:40</b>
TCP/IP Fingerprint OS Estimate: <b>Microsoft Windows</b>		Scan Expiration: <b>2012-01-26</b>

SecurityMetrics has determined that SIGMAALPHAEPSILON is COMPLIANT with the PCI scan validation requirement for this computer. Congratulations, the computer **passes** because no risk of 4 or more was found.

You may now use the SecurityMetrics Certified logo. Your Site Certification ID is: 699132. Please write this down and proceed to [Add Site Certified Logo Instructions](#).

Attackers typically use footprinting, port scanning and security vulnerability testing to find security weaknesses on computers. This report provides information on each of these categories.

## Footprinting

Find public information regarding this IP, which an attacker could use to gain access: [IP Information](#)

## Port Scan

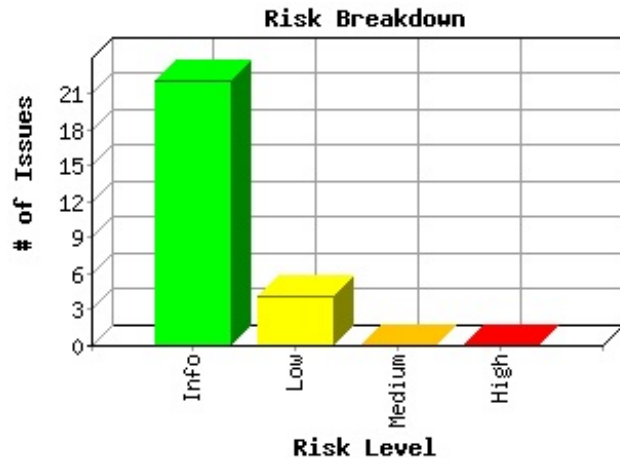
Attackers use a port scan to find out what programs are running on your computer. Most programs have known security weaknesses. Disable any unnecessary programs listed below.

Port Scan					
Protocol	Port	Program	Status	Summary	Turn Off
ICMP	Ping		Accepting	Your computer is answering ping requests. Hackers use Ping to scan the Internet to see if computers will answer. If your computer answers then a hacker will know your computer exists and your computer could become a hacker target. You should install a firewall or turn off Ping requests.	<a href="#">HowTo</a>
TCP	80	Microsoft IIS httpd 7.5	Open	Your computer appears to be running http software that allows others to view its web pages. If you don't intend this computer to allow others to view its web pages then turn this service off. There are many potential security vulnerabilities in http software.	<a href="#">HowTo</a>
TCP	443	Microsoft IIS httpd 7.5	Open	Your computer appears to be running HTTP Secure Socket Layer (SSL) software. This software improves the security of HTTP communication with this server.	

## Security Vulnerabilities Solution Plan

The following section lists all security vulnerabilities detected on your system. All vulnerability risk scores 4 or greater are marked in **red** and must be resolved to become PCI compliant. Denial-of-Service vulnerabilities are also marked in **red** but they do not affect your PCI compliance status. Each vulnerability is ranked on a scale from 0 to 10, with 10 being critical. [PCI Risk Table](#)

Security Vulnerabilities				
Protocol	Port	Program	Risk	Summary
TCP		http/https	<b>3</b>	Subdomain "incircle.sae.net" encountered but not scanned. For complete coverage, this and other subdomains may need to be scanned. This website may have other injection related vulnerabilities.
TCP	443	https	<b>2</b>	Description: Cookie transmitted over HTTPS without secure attribute Severity: Potential Problem CVE: <a href="#">CVE-2004-0462</a> Impact: Vulnerabilities in transmission of Cookie variables over HTTPS could lead to inappropriate information being transmitted in plaintext. Background: Cookies are a method of transmitting state information between web servers and clients. Resolution Apply a patch or upgrade from your vendor. Vulnerability Details: Service: https Received: Set-Cookie: ASP.NET_SessionId=0gzj21450owirqb4kb4ve355; path=/; HttpOnly?
				Description: SSL certificate is signed with weak hash function: SHA1 Severity: Potential Problem Impact: The SSL certificate is signed with a weak hash function. An attacker may be able to forge a SSL certificate that would appear to be valid for the website. This may allow the attacker perform a man-in-the-middle attack against the SSL-secured website. Background: Secure Sockets Layer (SSL) is an encryption



TCP	443	https	2	<p>protocol used to ensure data confidentiality, integrity, and authenticity during transit. It is commonly used between web browsers and web servers to protect sensitive data such as passwords and credit card numbers from being viewed by outsiders, modified in transit, or impersonated by unauthorized entities. The security provided by an SSL session comes through the use of encryption cyphers. Both parties participating in the session must exchange secret encryption key in clear text before the encrypted session. This must be done such that an eavesdropper is not able to intercept these keys during the exchange and use them to decipher the forthcoming messages. The mechanism by which this exchange occurs is through the use of securely signed encryption certificates. The signing of the certificates confirms that the content of the certificate has not been altered since it was originally produced by a trusted issuer, known as a Certificate Authority (CA). The signing process is performed by creating a hash signature of the certificate using a strong Cryptographic Hash Function (CHF). A CHF produces a fixed-length random signature for an arbitrary message of any length. A strong CHF will make it impossible to determine the original message given just the signature. It should also be unfeasibly difficult to create a message that produces a predetermined signature. However, given that the signature has a fixed length and the number of possible message combinations is endless, it is possible for a CHF to produce the same signature for two distinct messages. When this occurs, it is known as a hash collision. Ideally, in order to brute force a hash collision against a CHF that produces an output of n-bytes, it will take an attacker <math>2^n</math> iterations. If a mathematical attack is developed that allows the discovery of a hash collision using a CHF in a sufficiently short amount of time, then the security provided by the hash function has been compromised and it should no longer be used for cryptographic purposes. Resolution MD5 Hash Collision Vulnerability Sites using certificates signed using a vulnerable hash function should request replacement certificates signed with a more robust hash function. Currently, the SHA-256 and SHA-512 hash functions have proven to be resistant against both collision and preimage attacks. It is advisable to use one of these hash functions at this time. If this is not an acceptable risk, then the SHA1 hash may be used if the certificates are frequently revoked and replaced. Certificates signed using the SHA2 hash functions can be provided by most commercial CAs, given a Certificate Signing Request (CSR) that requires them. Additionally, OpenSSL and Microsoft IIS Certificate Services are capable of generating SHA2-signed certificates. If the SHA1 hash function is being used prior to December 31, 2010, it may continue to be used if the certificate is less than two years old. Older SHA1 certificates should be revoked and replaced with new certificates. If the replacement uses SHA1, it is recommended that the certificates expire in early 2011, such that they can be replaced with SHA2-signed certificates. Related Products Resolutions Cisco UWN 7 - Upgrade to Cisco UWN <b>Solution</b> 7.0.98.0 or newer. Vulnerability Details : Service: https OID: 0x2a864886f70d010105</p>
TCP	80	http	2	<p>Description: Flash application debugging output (/custom/CustomChapterMap.swf) Severity: Potential Problem Impact: The Flash application could potentially disclose sensitive information. Background: Adobe Flash is a platform for enhancing the content of web pages. Its capabilities include animation, video, and user interactivity. Flash applications are delivered to the browser as SWF (Small Web Format) files, which can include sound, graphics, and instruction code written in the ActionScript language. Resolution Remove calls to the trace() function from Flash applications on production servers. Vulnerability Details : Service: http found trace() call in ActionScript package [Global] class CustomChapterMap public function populateGrid(arg0:Object) { var loc7:* = null; var loc8:* = null; var loc0:* = arg0.name.split("_")[1]; var loc1:* = new Array(); trace(loc0); var loc2:* = 0; addTween(0.2, {"x":this.centerPointX, "y":this.centerPointY, "time":0.2}); var loc3:* = new DataProvider(); var loc4:* = new DataProvider(); var loc5:* = new DataProvider(); var loc6:* = new DataProvider(); this.dpChaptersPersist = new DataProvider();</p>
UDP		general/udp	0	<p>Synopsis : It was possible to obtain traceroute information. Description : Makes a traceroute to the remote host. <b>Solution:</b> n/a <b>Risk Factor:</b> None</p>
TCP		general/tcp	0	<p>Synopsis : It was possible to resolve the name of the remote host. Description : SMetrics was able to resolve the FQDN of the remote host. <b>Solution:</b> n/a <b>Risk Factor:</b> None</p>
TCP	443	https	0	<p>Synopsis : A web server is running on the remote host. Description : This plugin attempts to determine the type and the version of the remote web server. <b>Solution:</b> n/a <b>Risk Factor:</b> None</p>
TCP	443	https	0	<p>Synopsis : SMetrics crawled the remote web site. Description : This script makes a mirror of the remote web site(s) and extracts the list of CGIs that are used by the remote host. It is suggested that you change the number of pages to mirror in the 'Options' section of the client. <b>Solution:</b> n/a <b>Risk Factor:</b> None</p>
				<p>Here is the SSLv3 server certificate: Certificate: Data: Version: 3 (0x2) Serial Number: 59397 (0xe805) Signature Algorithm: sha1WithRSAEncryption Issuer: C=US, O=GeoTrust, Inc., CN=GeoTrust SSL CA Validity Not Before: Sep 27 23:58:35 2011 GMT Not After : Oct 29 13:53:07 2014 GMT Subject: serialNumber=lmAxGOxvi1dtwv-Z5U-ihoMQDABZ eo6V, C=US, ST=South Carolina, L=Charleston, O=Blackbaud Inc., OU=Hosting Services, CN=www.sae.net Subject Public Key Info: Public Key Algorithm: rsaEncryption RSA Public Key: (2048 bit) Modulus (2048 bit): 00:af:53:39:96:34:f5:9d:36:2e:c8:79:0e:fd :bd:d4:69:53:b4:28:2c:65:e9:49:cc:9d:4d:40:23 :e9:7b:84:f2:73:06:58:9f:ae:be:b0:29:60:ac:91 :5c:</p>

TCP	443	https	<p>6c:03:e7:86:5b:1c:e5:52:f8:8a:78:a6:7a:ca :58:16:45:d2:2d:93:71:b0:6e:45:69:29:2e:74:f9 :d6:ec:c4:99:47:24:27:d2:87:6a:36:01:67:86:b1 :41:69:8b:8b:6f:4f:e3:3e:71:9a:11:17:62:1e:66 :d6:4c:e5:c9:66:b2:25:4f:49:e1:74:d4:f2:d2:01 :11:a8:43:96:3f:5b:04:eb:f3:4c:b1:34:2d:f3:0b :4a:c5:b6:56:1b:e0:1e:ba:93:d7:aa:38:af:87:62 :01:bb:e1:da:7f:79:ae:f9:fa:35:62:1c:92:31:76 :17:52:7a:b1:a6:71:a4:9a:7b:16:87:96:bf:4c:69 :8b:22:bc:d5:31:dd:78:18:d2:b3:1f:b4:4e:9d:ba :a5:82:4a:a4:85:3d:d1:29:11:d6:68:a4:c5:7c:35 :eb:60:e2:0d:bf:9d:57:9e:d9:0f:26:6c:42:74:ca :a7:00:f3:20:61:ae:b6:71:33:48:52:c2:ef:9e:73 :bc:22:a0:23:5f:60:81:f8:c2:d7:45:80:a2:05:80 :0c: 58:df Exponent: 65537 (0x10001)</p> <p><b>0</b> X509v3 extensions: X509v3 Authority Key Identifier: keyid:42:79:54:1B:61:CD:55:2B:3E:63:D5:3C :48:57:F5:9F:FB:45:CE:4A X509v3 Key Usage: critical Digital Signature, Key Encipherment, Data Encipherment X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication X509v3 Subject Alternative Name: DNS:www.sae.net, DNS:sae.net X509v3 CRL Distribution Points: URI:<a href="http://qtssl-crl.geotrust.com/crls/gtssl.crl">http://qtssl-crl.geotrust.com/crls/gtssl.crl</a> X509v3 Subject Key Identifier: F7:A5:AB:E1:4A:92:3A:3F:6D:08:80:0C:80:90 :FD:6E:13:F4:98:CF X509v3 Basic Constraints: critical CA:FALSE Authority Information Access: CA Issuers - URI:<a href="http://qtssl-aia.geotrust.com/qtssl.crt">http://qtssl-aia.geotrust.com/qtssl.crt</a> Signature Algorithm: sha1WithRSAEncryption 38:d8:ab:60:09:6b:13:3c:7f:4c:ea:a4:3c:7c :81:0b:43:ab:0c:24:b5:7c:b2:03:0a:2e:60:bd:e6:ab:5d:07 :cf:73:ab:89:c1:8c:35:41:ac:75:5c:5a:a6:b2:9a:92:22:0c :ec:9e:f3:06:06:e3:3a:57:0c:0c:0d:a8:27:47:68:e6:1e:a9 :fa:83:ba:60:f9:d0:66:dd:81:5c:5f:2f:c0:a5:b6:d3:4a:0f :00:20:13:3d:bc:93:46:2b:57:f5:ad:02:8f:62:bf:2a:7a:e4 :78:5c:94:bc:5c:b1:a6:53:02:fe:cf:fa:82:12:19:0d:cd:ed :38:48:3e:03:18:2c:e0:87:47:b7:ff:dc:27:84:c0:c6:4a:f1 :8a:e1:28:72:c3:5e:e2:87:09:c1:5b:5e:b6:4e:e6:51:e8:e0 :a6:44:15:67:22:0b:40:90:52:4c:a2:7a:0b:4c:7b:7e:9f:f0 :0a:85:b3:22:7a:36:d5:4b:3f:5a:32:d7:49:ab:8a:50:27:bb :b7:34:b9:6c:4c:38:76:97:2a:f0:59:d9:c4:f5:57:f3:f8:66 :74:65:0c:df:6f:27:31:76:1a:c0:d6:4a:e2:45:18:04:d5:0e :82:df:9a:8a:4b:54:c3:b0:fc:5d:8a:58:e0:8d:5e:67:5f:04 :28:c7:59:32: 75:1d:1e:8f This SSLv3 server does not accept SSLv2 connections. This SSLv3 server also accepts TLSv1 connections.</p>
TCP	443	https	<p><b>0</b> Synopsis : It is possible to retrieve file backups from the remote web server. Description : By appending various suffixes (ie: .old, .bak, ~, etc...) to the names of various files on the remote host, it seems possible to retrieve their contents, which may result in disclosure of sensitive information. See also : <a href="http://projects.webappsec.org/Predictable-Resource-Location">http://projects.webappsec.org/Predictable-Resource-Location</a> <b>Solution:</b> Ensure the files do not contain any sensitive information, such as credentials to connect to a database, and delete or protect those files that should not be accessible. <b>Risk Factor:</b> Medium / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)</p>
TCP	443	https	<p><b>0</b> Synopsis : HMAP fingerprints the remote HTTP server. Description : By sending several valid and invalid HTTP requests, it may be possible to identify the remote web server type. In some cases, its version can also be approximated, as well as some options. An attacker may use this tool to identify the kind of the remote web server and gain further knowledge about this host. Suggestions for defense against fingerprinting are presented in <a href="http://acsac.org/2002/abstracts/96.html">http://acsac.org/2002/abstracts/96.html</a> See also : <a href="http://ujeni.murkyroc.com/hmap/">http://ujeni.murkyroc.com/hmap/</a> <a href="http://seclab.cs.ucdavis.edu/papers/hmap-thesis.pdf">http://seclab.cs.ucdavis.edu/papers/hmap-thesis.pdf</a> <a href="http://projects.webappsec.org/Fingerprinting">http://projects.webappsec.org/Fingerprinting</a> <b>Solution:</b> n/a <b>Risk Factor:</b> None</p>
TCP	443	https	<p><b>0</b> Synopsis : This plugin performs service detection. Description : This plugin is a complement of find_service1.nasl. It attempts to identify common services which might have been missed because of a network problem. <b>Solution:</b> See below <b>Risk Factor:</b> None</p>
TCP	443	https	<p><b>0</b> Synopsis : The remote service encrypts communications using SSL. Description : This script detects which SSL ciphers are supported by the remote service for encrypting communications. See also : <a href="http://www.openssl.org/docs/apps/ciphers.html">http://www.openssl.org/docs/apps/ciphers.html</a> <b>Solution:</b> n/a <b>Risk Factor:</b> None</p>
TCP	443	https	<p><b>0</b> Synopsis : Some information about the remote HTTP configuration can be extracted. Description : This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc... This test is informational only and does not denote any security problem. <b>Solution:</b> n/a <b>Risk Factor:</b> None</p>
TCP	443	https	<p><b>0</b> path = / name = NSC_QH-28013 value = ffffffff090c357f45525d5f4f58455e445a4a42378b version = 1 httponly = 1 path = / name = VisitorGuid value = 6b01f0d6-f7d3-444a-9396-8f1be591c89e version = 1 expires = Fri, 28-Oct-2061 10:39:16 GMT path = / name = ASP.NET_SessionId value = jkqf0w55wmsukg55oqy5df2y version = 1 httponly = 1</p>
			<p>Synopsis : This plugin determines which HTTP methods are allowed on various CGI directories. Description : By calling the OPTIONS method, it is possible to determine</p>

TCP	443	https	0	which HTTP methods are allowed on each directory. As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501. Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities. <b>Solution:</b> n/a <b>Risk Factor:</b> None
TCP	443	https	0	Synopsis : Links to external sites were gathered. Description : SMetrics gathered HREF links to external sites by crawling the remote web server. <b>Solution:</b> n/a <b>Risk Factor:</b> None
TCP	80	http	0	Synopsis : A web server is running on the remote host. Description : This plugin attempts to determine the type and the version of the remote web server. <b>Solution:</b> n/a <b>Risk Factor:</b> None
TCP	80	http	0	Synopsis : SMetrics crawled the remote web site. Description : This script makes a mirror of the remote web site(s) and extracts the list of CGIs that are used by the remote host. It is suggested that you change the number of pages to mirror in the 'Options' section of the client. <b>Solution:</b> n/a <b>Risk Factor:</b> None
TCP	80	http	0	Synopsis : It is possible to retrieve file backups from the remote web server. Description : By appending various suffixes (ie: .old, .bak, ~, etc...) to the names of various files on the remote host, it seems possible to retrieve their contents, which may result in disclosure of sensitive information. See also : <a href="http://projects.webappsec.org/Predictable-Resource-Location">http://projects.webappsec.org/Predictable-Resource-Location</a> <b>Solution:</b> Ensure the files do not contain any sensitive information, such as credentials to connect to a database, and delete or protect those files that should not be accessible. <b>Risk Factor:</b> Medium / CVSS Base Score : 5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)
TCP	80	http	0	Synopsis : HMAP fingerprints the remote HTTP server. Description : By sending several valid and invalid HTTP requests, it may be possible to identify the remote web server type. In some cases, its version can also be approximated, as well as some options. An attacker may use this tool to identify the kind of the remote web server and gain further knowledge about this host. Suggestions for defense against fingerprinting are presented in <a href="http://acsac.org/2002/abstracts/96.html">http://acsac.org/2002/abstracts/96.html</a> See also : <a href="http://ujeni.murkyroc.com/hmap/">http://ujeni.murkyroc.com/hmap/</a> <a href="http://seclab.cs.ucdavis.edu/papers/hmap-thesis.pdf">http://seclab.cs.ucdavis.edu/papers/hmap-thesis.pdf</a> <a href="http://projects.webappsec.org/Fingerprinting">http://projects.webappsec.org/Fingerprinting</a> <b>Solution:</b> n/a <b>Risk Factor:</b> None
TCP	80	http	0	Synopsis : This plugin performs service detection. Description : This plugin is a complement of find_service1.nasl. It attempts to identify common services which might have been missed because of a network problem. <b>Solution:</b> See below <b>Risk Factor:</b> None
TCP	80	http	0	Synopsis : Some information about the remote HTTP configuration can be extracted. Description : This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc... This test is informational only and does not denote any security problem. <b>Solution:</b> n/a <b>Risk Factor:</b> None
TCP	80	http	0	path = / name = NSC_QH-28013 value = ffffffff090c357f45525d5f4f58455e445a4a423660 version = 1 httponly = 1 path = / name = VisitorGuid value = 16240d5a-44db-4d3a-9af5-a4aa9a65f735 version = 1 expires = Fri, 28-Oct-2061 10:39:07 GMT path = / name = ASP.NET_SessionId value = tqz14k45a1ghsbf2loulydvd version = 1 httponly = 1
TCP	80	http	0	Synopsis : This plugin determines which HTTP methods are allowed on various CGI directories. Description : By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory. As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes' in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501. Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities. <b>Solution:</b> n/a <b>Risk Factor:</b> None
TCP	80	http	0	Synopsis : Links to external sites were gathered. Description : SMetrics gathered HREF links to external sites by crawling the remote web server. <b>Solution:</b> n/a <b>Risk Factor:</b> None

For a list of all vulnerabilities in our knowledge base on this test date [click here](#).

CONFIDENTIAL AND PROPRIETARY INFORMATION  
SECURITYMETRICS PROVIDES THIS INFORMATION "AS IS" WITHOUT ANY WARRANTY OF ANY KIND. SECURITYMETRICS MAKES NO WARRANTY THAT THESE SERVICES WILL DETECT EVERY VULNERABILITY ON YOUR COMPUTER, OR THAT THE SUGGESTED SOLUTIONS AND ADVICE PROVIDED IN THIS REPORT, TOGETHER WITH THE RESULTS OF THE VULNERABILITY ASSESSMENT, WILL BE ERROR-FREE OR COMPLETE. SECURITYMETRICS SHALL NOT BE RESPONSIBLE OR LIABLE FOR THE ACCURACY, USEFULNESS, OR AVAILABILITY OF ANY INFORMATION TRANSMITTED VIA THE SECURITYMETRICS SERVICE, AND SHALL NOT BE RESPONSIBLE OR LIABLE FOR ANY USE OR APPLICATION OF THE INFORMATION CONTAINED IN THIS REPORT. DISSEMINATION, DISTRIBUTION, COPYING OR USE OF THIS DOCUMENT IN WHOLE OR IN PART BY A SECURITYMETRICS COMPETITOR OR THEIR AGENTS IS STRICTLY PROHIBITED.

This report was generated by a PCI Approved Scanning Vendor, SecurityMetrics, Inc., under certificate number 3707-01-

06, within the guidelines of the PCI data security initiative.