McAfee | McAfee SECURE™

PCI Security Report

Adobe Business Catalyst

Report Generation Date:03-DEC-2010 22:40

Confidential Information
The following report contains confidential information. Do not distribute, email, fax or transfer via any electric mechanism unless it has been approved by your organization's security policy. All copies and backups of this document should be maintained on protected storage at all times. Do not share any of the information contained within this report with anyone unless you confirm they are authorized to view the information.

Disclaimer
This, or any other, vulnerability audit cannot and does not guarantee security. McAfee makes no warranty or claim of any kind, whatsoever, about the accuracy or usefulness of any information provided herein. By using this information you agree that McAfee shall be held harmless in any event. McAfee makes this information available solely under its Terms of Service Agreement published at www.mcafeesecure.com.

Disclosure
As a systems and networks security company, McAfee produces and sells a range of products separately from services provided as an Approved Scanning Vendor. McAfee security products include but may not be limited to the following categories: application or network firewalls, intrusion detection/prevention, database or other encryption solutions, security audit log solutions, anti-virus solutions

Table Of Contents	
Section	
1	Executive Summary
2	Certification of Regulatory Compliance
3.1	Device: 69.20.239.62
3.1.1	Overview
3.1.2	Open Ports
3.1.3	Consolidated Solution
3.1.4	Vulnerabilities
3.1.5	Resolved
3.2	Device: 83.231.190.50
3.2.1	Overview
3.2.2	Open Ports
3.2.3	Consolidated Solution
3.2.4	Vulnerabilities
3.2.5	Resolved
3.3	Device: 192.150.2.140 / nj.worldsecuresystems.com (192.150.2.140)
3.3.1	Overview
3.3.2	Open Ports
3.3.3	Consolidated Solution
3.3.4	Vulnerabilities
3.3.5	Resolved
3.4	Device: 202.176.14.137 / syd.worldsecuresystems.com (202.176.14.137)
3.4.1	Overview
3.4.2	Open Ports
3.4.3	Consolidated Solution
3.4.4	Vulnerabilities
3.4.5	Resolved

Executive Summary

McAfee has determined that 'Adobe Business Catalyst' is **COMPLIANT** with the PCI scan validation requirement.

This report was generated by PCI Approved scanning vendor, McAfee, under certificate number 3709-01-04 in the framework of the PCI data security initiative.

As a Qualified Independent Scan Vendor McAfee is accredited by Visa, MasterCard, American Express, Discover Card and JCB to perform network security audits conforming to the Payment Card Industry (PCI) Data Security Standards.

To earn validation of PCI compliance, network devices being audited must pass tests that probe all of the known methods hackers use to access private information, in addition to vulnerabilities that would allow malicious software (i.e. viruses and worms) to gain access to or disrupt the network devices being tested.

NOTE: In order to demonstrate compliance with the PCI Data Security Standard a vulnerability scan must have been completed within the past 90 days with no vulnerabilities listed as URGENT, CRITICAL or HIGH (numerical severity ranking of 3 or higher) present on any device within this report. Additionally, Visa and MasterCard regulations require that you configure your scanning to include all IP addresses, domain names, DNS servers, load balancers, firewalls or external routers used by, or assigned to, your company, and that you configure any IDS/IPS to not block access from the originating IP addresses of our scan servers.

Certification of Regulatory Compliance

Sites are tested and certified daily to meet all U.S. Government requirements for remote vulnerability testing as set forth by the National Infrastructure Protection Center (NIPC). They are also certified to meet the security scanning requirements of Visa USA's Cardholder Information Security Program (CISP), Visa International's Account Information Security (AIS) program, MasterCard Internationals's Site Data Protection (SDP) program, American Express' CID security program, the Discover Card Information Security and Compliance (DISC) program within the framework of the Payment Card Industry (PCI) Data Security Standard.

3.1.1 - Overview: 69.20.239.62

Scan Date	1	2	3	4	5
03-DEC-2010 22:31	11	0	0	0	0

3.1.2 - Open Ports: 69.20.239.62

Port	Protocol	Service	Banner
21	tcp	ftp	ftp
80	tcp	http	http
443	tcp	https	https

3.1.3 - Consolidated Solution: 69.20.239.62

All level 3, 4, and 5 vulnerabilities identified for this device must be addressed with mitigation or remediation in order to satisfy PCI requirements.
Review all findings for this device, then for each vulnerability with level 3, 4, or 5, implement the solution described or an equivalent solution. Regenerate and submit the report based on scan results taken after remediation is completed.
If mitigations are employed according to the compensating controls mechanism of PCI, you must provide details of compensating controls for each level 3, 4, or 5 vulnerability that appears in this report.

3.1.4 - Vulnerabilities: 69.20.239.62

Severity	Name	Port	Category	Status
1	SSL Cert Mismatch	443/tcp	Web Server	Pass

Description

The SSL certificate does NOT match the website. This may prevent users from trusting/validating the website or service.
Example, if the SSL certificate has been issued for [www.paypal.com] and the site is accessed via [paypal.com]; the user will receive the following security warning.

"The security certificate presented by this website was issued for a different website's address."

CVSS Score

0.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution

Contact the web administrator to correct/create a new SSL certificate using the correct website name.

Details

Subject(s) on cert do(es) not match target host { Target Host : SubjectCN(s) }. {69.20.239.62 : *.worldsecuresystems.com}

Links

SSL Certificates - Security Certificate Errors

References

None

Severity	Name	Port	Category	Status
1	SSL Cert Info	443/tcp	Web Server	Pass

Description

This test attempts to provide details pertaining to your SSL certificate.

CVSS Score

0.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution

None

Details

%3C%3Fxml+version%3D%221.0%22+encoding%3D%22UTF-
8%22+standalone%3D%22no%22%3F%3E%3Csslreport%3E%3Ccertificate+expired%3D%22false%22%3E%3
Csubject%3ECN%3D*.worldsecuresystems.com%2C+O%3D*.worldsecuresystems.com%2C+OU%3DDomain+
Control+Validated%2C+C%3DUS%3C%2Fsubject%3E%3Cissuer%3ECN%3DGlobalSign+Domain+Validation+
CA%2C+O%3DGlobalSign+nv-
sa%2C+OU%3DDomain+Validation+CA%2C+C%3DBE%3C%2Fissuer%3E%3Cserial_number%3E1208925819
615913170207512%3C%2Fserial_number%3E%3Csignature_algorithm%3ESHA1withRSA%3C%2Fsignature_a
lgorithm%3E%3Cfrom_date%3EWed+Sep+08+17%3A27%3A26+PDT+2010%3C%2Ffrom_date%3E%3Cto_dat
e%3EFri+Sep+09+17%3A27%3A23+PDT+2011%3C%2Fto_date%3E%3Cversion%3E2%3C%2Fversion%3E%
3Cpublic_key%3ESun+RSA+public+key%2C+2048+bits%3C%2Fpublic_key%3E%3C%2Fcertificate%3E%3Cce
rtificate+expired%3D%22false%22%3E%3Csubject%3ECN%3DGlobalSign+Domain+Validation+CA%2C+O%3
DGlobalSign+nv-
sa%2C+OU%3DDomain+Validation+CA%2C+C%3DBE%3C%2Fsubject%3E%3Cissuer%3ECN%3DGlobalSign
+Root+CA%2C+OU%3DRoot+CA%2C+O%3DGlobalSign+nv-
sa%2C+C%3DBE%3C%2Fissuer%3E%3Cserial_number%3E48357032784597462111995 32%3C%2Fserial_nu
mber%3E%3Csignature_algorithm%3ESHA1withRSA%3C%2Fsignature_algorithm%3E%3Cfrom_date%3EFri+
May+04+03%3A00%3A00+PDT+2007%3C%2Ffrom_date%3E%3Cto_date%3EThu+May+04+05%3A00%3A00
+PDT+2017%3C%2Fto_date%3E%3Cversion%3E2%3C%2Fversion%3E%3Cpublic_key%3ESun+RSA+public+
key%2C+2048+bits%3C%2Fpublic_key%3E%3C%2Fcertificate%3E%3Cssl_cert_mismatch%3Efalse%3C%2Fs
sl_cert_mismatch%3E%3Cssl_cert_self_signed%3Efalse%3C%2Fssl_cert_self_signed%3E%3Cnegotiated_prot
ocol%3ETLSv1%3C%2Fnegotiated_protocol%3E%3Cnegotiated_cipher%3ETLS_RSA_WITH_AES_128_CBC_
SHA%3C%2Fnegotiated_cipher%3E%3Cserver_enabled_cipher%3ETLS_RSA_WITH_AES_128_CBC_SHA%3
C%2Fserver_enabled_cipher%3E%3C%2Fsslreport%3E

Links

None

References

None

Severity	Name	Port	Category	Status
1	Missing Secure Attribute in an Encrypted Session (SSL) Cookie	443/tcp	Web Application	Pass

Description

The application sets a cookie over a secure channel without using the "secure" attribute. RFC states that if the cookie does not have the secure attribute assigned to it, then the cookie can be passed to the server by the client over non-secure channels (http). Using this attack, an attacker may be able to intercept this cookie, over the non-secure channel, and use it for a session hijacking attack.

CVSS Score

2.1

CVSS Fingerprint

AV:L/AC:L/Au:N/C:P/I:N/A:N

Solution

It is best business practice that any cookies that are sent (set-cookie) over an SSL connection to explicitly state secure on them.

Details

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							

Path: / --> No "Secure" Attribute on Secure Channel (https) : ASP.NET_SessionId=fwvciq551nzddeyy1axsraai; path=/; HttpOnly

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							

Path: / --> No "Secure" Attribute on Secure Channel (https) : ASP.NET_SessionId=hsy4jf45nkmvvu2ifegd31qb; path=/; HttpOnly

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							
Headers	Host=69.20.239.62							

Path: / --> No "Secure" Attribute on Secure Channel (https) : ASP.NET_SessionId=wnwnp0rpsv2muo45xh1ecd45; path=/; HttpOnly

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							
Headers	Host=69.20.239.62							

Path: / --> No "Secure" Attribute on Secure Channel (https) : ASP.NET_SessionId=xxlp5zfkjdbunb55xx3apv55; path=/; HttpOnly

Links

owasp
RFC 2109 - HTTP State Management Mechanism
Persistent Client State HTTP Cookies

References

CVE CVE-2004-0462
Open Source Vulnerability Database 19183

Severity	Name	Port	Category	Status
1	Potentially Sensitive Information Missing Secure Attribute in an Encrypted Session (SSL) Cookie	443/tcp	Web Application	Pass

Description

The application sets a cookie over a secure channel without using the "secure" attribute. RFC states that if the cookie does not have the secure attribute assigned to it, then the cookie can be passed to the server by the client over non-secure channels (http). Using this attack, an attacker may be able to intercept this cookie, over the non-secure channel, and use it for a session hijacking attack.

The information that was sent was flagged as being potentially sensitive. Potentially sensitive information could be session tokens, user id's, or passwords.

CVSS Score

2.1

CVSS Fingerprint

AV:L/AC:L/Au:N/C:P/I:N/A:N

Solution

It is best business practice that any cookies that are sent (set-cookie) over an SSL connection to explicitly state secure on them. Speak with your web developer to have them enable the secure attribute on cookies sent over secure connections.

Details

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							

Path: / --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=fwvciq551nzddeyy1axsraai; path=/; HttpOnly

Protocol	https	**Port**	443	**Read Timeout**	10000	**Method**	GET	Demo
Path	/							

Path: / --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=hsy4jf45nkmvvu2ifegd31qb; path=/; HttpOnly

Protocol	https	**Port**	443	**Read Timeout**	10000	**Method**	GET	Demo
Path	/							
Headers	Host=69.20.239.62							

Path: / --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=wnwnp0rpsv2muo45xh1ecd45; path=/; HttpOnly

Protocol	https	**Port**	443	**Read Timeout**	10000	**Method**	GET	Demo
Path	/							
Headers	Host=69.20.239.62							

Path: / --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=xxlp5zfkjdbunb55xx3apv55; path=/; HttpOnly

Links

CWE.Mitre.org
Persistent Client State HTTP Cookies
CVE..Mitre.org
RFC 2109 - HTTP State Management Mechanism

References

CVE CVE-2004-0462

Severity	Name	Port	Category	Status
1	SSL Cipher Suites Supported	443/tcp	Web Application	Pass

Description

This script detects which SSL ciphers are supported by the remote service for encrypting communications.

CVSS Score

2.6

CVSS Fingerprint

AV:N/AC:H/Au:N/C:P/I:N/A:N

Solution

Ensure that your server is capable of supporting the latest and strongest strength ciphers. Keeping your server patched and updated is helpful.

For more information view the openssl link below.

Details

Here is the list of SSL ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)
SSLv3
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}

Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

Links

www.openssl.org/docs/apps/ciphers.html

References

None

Severity	Name	Port	Category	Status
1	SSL Certificate Information	443/tcp	Web Server	Pass

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

CVSS Score

0.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution

Please disable if you have any low strength ciphers

Details

Subject Name:

Country: US
Organization Unit: Domain Control Validated
Organization: *.worldsecuresystems.com
Common Name: *.worldsecuresystems.com

Issuer Name:

Country: BE
Organization Unit: Domain Validation CA
Organization: GlobalSign nv-sa
Common Name: GlobalSign Domain Validation CA

Serial Number: 01 00 00 00 00 01 2A F4 18 83 18

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Sep 09 00:27:26 2010 GMT
Not Valid After: Sep 10 00:27:23 2011 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 C5 EE 8B C9 C9 A2 62 E5 74 A4 DE FD 6B 63 C6 24 8F A0 7A
EC A0 6F BD 13 DB 5D 1C 66 53 A7 CF DF 4B 40 02 93 6B B2 04
CB 30 E6 0A F6 44 F1 96 C8 8B E0 CE DD 64 F8 D3 B1 1C 1F F4
08 50 A3 F3 73 03 DE 5C 7F 40 77 55 73 72 A8 79 48 9D 22 F9
24 D6 F4 CD DA 60 3D E3 3E 4D 99 24 2E B9 76 D9 EC 8B 80 54
6C 47 E2 60 13 F6 C7 E7 D3 F1 89 F5 DA B1 A0 E4 05 CC 21 7F
53 80 EA 0C 47 20 61 41 6E AB FF E7 D5 47 0F 5C 98 93 27 C7
70 38 39 A2 42 A4 BE 83 0E F6 3C 7D B0 05 1C F3 5D 53 65 90
51 41 EC 51 68 37 F2 4F 4D 79 A3 BE AC 55 00 4A 81 EC 14 C0
F6 E8 6B 80 98 2B E5 BC 2D 25 14 EE 06 D5 21 E0 C0 0F C0 E4
56 6A AF 87 E0 D1 7D B2 11 D9 79 70 48 55 BA 03 D4 18 D0 1A
DD C5 8C FF 5C 6C D2 F5 2C 98 19 5B C9 F4 65 DC 98 FB 24 D2
36 8D F9 E6 42 B5 3E 23 C7 82 16 FC 5B B5 91 75 FF

Exponent: 01 00 01

Signature: 00 0F DD 5D 8A 26 D7 F3 EE DC C8 86 EF D7 D1 23 A6 C7 E6 F2
29 45 EC B2 F9 F0 DE 4E A1 F4 D4 33 DB EB 3C EA A1 3D D2 76
E5 EB EA 93 3B E4 0B 1A 7F B9 45 F8 FF 4D C9 E0 F5 9E 30 F6
7C 65 A1 AD 80 ED 60 1F EB A7 96 EB 1E D1 77 E8 31 3A 44 1B
42 86 62 60 F5 83 11 09 A7 C1 DB 90 29 B9 04 D6 88 66 7F 65
13 CE 16 E4 56 50 3D CE D9 3C D7 FD 2D 81 F0 74 03 65 35 4F
E6 C4 7D 38 E9 E4 C4 AA 50 A3 34 B9 2B F6 FA 3E 87 9C E8 F6
B4 40 8D 62 2C F6 A6 B1 1F 9E FB 4D 35 3F CB 6B 17 9F E4 25
DE 10 3B 6B C6 1A F0 DE A3 34 0E 1D EB A1 B4 8F 79 4C 2C BC
D9 14 00 B2 B5 55 ED 4B A1 84 39 6B A9 74 CD 4C 7B E1 31 D3
D0 1C 62 E8 92 CA 29 2F 05 AE 06 8C A2 99 2F 17 F3 3C 53 E1
5A 89 01 4E F1 D2 14 58 3C 42 55 78 93 67 A3 78 34 7F 80 18
BE 41 69 F7 5C 73 A0 16 E7 4E 84 5C 39 0B 24 2E 3F

Extension: Authority Key Identifier (2.5.29.35)
Critical: 0

Extension: Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical: 0
Method#1: Certificate Authority Issuers
URI: http://secure.globalsign.net/cacert/dvhe1.crt

Extension: CRL Distribution Points (2.5.29.31)
Critical: 0
URI: http://crl.globalsign.net/DomainVal1.crl

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: CB 94 6E A1 E6 3D 08 F7 B9 4B 04 0B 53 B6 25 B4 F7 BF 15 C3

Extension: Basic Constraints (2.5.29.19)
Critical: 0
Data: 30 00

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment

Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2)
Purpose#3: Microsoft Server Gated Crypto (SGC) (1.3.6.1.4.1.311.10.3.3)

Extension: Policies (2.5.29.32)
Critical: 0
Policy ID #1: 1.3.6.1.4.1.4146.1.10
Qualifier ID #1: Certification Practice Statement (1.3.6.1.5.5.7.2.1)
CPS URI: http://www.globalsign.net/repository/

Extension: 2.16.840.1.113730.1.1
Critical: 0
Data: 03 02 06 C0

Extension: Subject Alternative Name (2.5.29.17)
Critical: 0
DNS: *.worldsecuresystems.com
DNS: worldsecuresystems.com

Links

Transport Layer Security
SSL 2.0
IBM HTTP Server
Disabling SSLv2 in IIS (English)
Mozillazine

References

None

Severity	Name	Port	Category	Status
1	Potentially Sensitive Information Missing Secure Attribute in an Encrypted Session (SSL) Cookie	80/tcp	Web Application	Pass

Description

The application sets a cookie over a secure channel without using the "secure" attribute. RFC states that if the cookie does not have the secure attribute assigned to it, then the cookie can be passed to the server by the client over non-secure channels (http). Using this attack, an attacker may be able to intercept this cookie, over the non-secure channel, and use it for a session hijacking attack.

The information that was sent was flagged as being potentially sensitive. Potentially sensitive information could be session tokens, user id's, or passwords.

CVSS Score

2.1

CVSS Fingerprint

AV:L/AC:L/Au:N/C:P/I:N/A:N

Solution

It is best business practice that any cookies that are sent (set-cookie) over an SSL connection to explicitly state secure on them. Speak with your web developer to have them enable the secure attribute on cookies sent over secure connections.

Details

Protocol http **Port** 80 **Read Timeout** 10000 **Method** GET Demo
Path /

Path: / --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=xyjxqxaewwu3mk45iuqlhfjk; path=/; HttpOnly

Protocol http **Port** 80 **Read Timeout** 90000 **Method** GET Demo
Path /BACLIENT

Path: /BACLIENT --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=jeq1x5bqm5xunnzqhisnzlaa; path=/; HttpOnly

Protocol http **Port** 80 **Read Timeout** 10000 **Method** GET Demo
Path /

Path: / --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=p4pl5v45nbe0ll55hmmrqwzj; path=/; HttpOnly

Protocol http **Port** 80 **Read Timeout** 10000 **Method** GET Demo
Path /

Path: / --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=qgas1k55uodbvw45annyrn55; path=/; HttpOnly

Links

CWE.Mitre.org
Persistent Client State HTTP Cookies
CVE..Mitre.org
RFC 2109 - HTTP State Management Mechanism

References

CVE CVE-2004-0462

Severity	Name	Port	Category	Status
1	FTP Supports Clear Text Authentication	21/tcp	FTP	Pass

Description

The remote FTP server allows the user's name and password to be transmitted in clear text, which may be intercepted by a network sniffer, or a man-in-the-middle attack.

CVSS Score

2.6

CVSS Fingerprint

AV:N/AC:H/Au:N/C:P/I:N/A:N

Solution

Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server such that control connections are encrypted.

Details

:

This FTP server does not support 'AUTH TLS'.
Other references : CWE:522, CWE:523

Links

Configuring & Using SSH/SFTP
Configuring vsftpd for Secure Connections
Setting up ProFTPd & TLS on Debian Etch
Filezilla - Free (GPL) FTP(S) & SFTP Client (Windows, Linux, OS X)

References

None

Severity	Name	Port	Category	Status
1	FTP Server Detection	21/tcp	FTP	Pass

Description

It is possible to obtain the banner of the remote FTP server by connecting to the remote port.

CVSS Score

0.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution

N/A

Details

The remote FTP banner is :

220-**********

220-Welcome to FTP

220-Please use your email address and password to login.

220-If you are registered for more than one site then your login name must be:
yourcompany.com/you@youremail.com.

220-**********

220-

220 FTP Server Ready

Links

None

References

None

Severity	Name	Port	Category	Status
1	TCP Timestamps	All	Other	Pass

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

CVSS Score

0.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution

n/a

Details

Synopsis :

The remote service implements TCP timestamps.

Description :

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See also :

http://www.ietf.org/rfc/rfc1323.txt

Solution :

n/a

Risk factor :

None

Links

www.ietf.org/rfc/rfc1323.txt

References

None

Severity	Name	Port	Category	Status
1	OS Identification	All	Other	Pass

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc...) it is possible to guess the name of the remote operating system in use, and sometimes its version

CVSS Score

0.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution

By modifying the banners of the services running and blocking ICMP requests at the firewall, OS fingerprinting can be limited.

Details

Synopsis :

It is possible to guess the remote operating system

Description :

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc...)
it is possible to guess the name of the remote operating system in use, and
sometimes its version

Solution :

N/A

Risk factor :

None

Plugin output :

Remote operating system : Microsoft Windows Server 2008
Confidence Level : 75
Method : HTTP

The remote host is running Microsoft Windows Server 2008

Links

None

References

None

3.1.5 - Resolved: 69.20.239.62

None

3.2.1 - Overview: 83.231.190.50

Scan Date	1	2	3	4	5
03-DEC-2010 22:35	5	0	0	0	0

3.2.2 - Open Ports: 83.231.190.50

Port	Protocol	Service	Banner
21	tcp	ftp	ftp
80	tcp	http	http
443	tcp	https	https

3.2.3 - Consolidated Solution: 83.231.190.50

All level 3, 4, and 5 vulnerabilities identified for this device must be addressed with mitigation or remediation in order to satisfy PCI requirements.
Review all findings for this device, then for each vulnerability with level 3, 4, or 5, implement the solution described or an equivalent solution. Regenerate and submit the report based on scan results taken after remediation is completed.
If mitigations are employed according to the compensating controls mechanism of PCI, you must provide details of compensating controls for each level 3, 4, or 5 vulnerability that appears in this report.

3.2.4 - Vulnerabilities: 83.231.190.50

Severity	Name	Port	Category	Status
1	SSL Cert Mismatch	443/tcp	Web Server	Pass

Description

The SSL certificate does NOT match the website. This may prevent users from trusting/validating the website or service.
Example, if the SSL certificate has been issued for [www.paypal.com] and the site is accessed via [paypal.com]; the user will receive the following security warning.

"The security certificate presented by this website was issued for a different website's address."

CVSS Score

0.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution

Contact the web administrator to correct/create a new SSL certificate using the correct website name.

Details

Subject(s) on cert do(es) not match target host { Target Host : SubjectCN(s) }. {83.231.190.50 : *.worldsecuresystems.com}

Links

SSL Certificates - Security Certificate Errors

References

None

Severity	Name	Port	Category	Status
1	SSL Cert Info	443/tcp	Web Server	Pass

Description

This test attempts to provide details pertaining to your SSL certificate.

CVSS Score

0.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution

None

Details

%3C%3Fxml+version%3D%221.0%22+encoding%3D%22UTF-
8%22+standalone%3D%22no%22%3F%3E%3Csslreport%3E%3Ccertificate+expired%3D%22false%22%3E%3
Csubject%3ECN%3D*.worldsecuresystems.com%2C+O%3D*.worldsecuresystems.com%2C+OU%3DDomain+
Control+Validated%2C+C%3DUS%3C%2Fsubject%3E%3Cissuer%3ECN%3DGlobalSign+Domain+Validation+
CA%2C+O%3DGlobalSign+nv-
sa%2C+OU%3DDomain+Validation+CA%2C+C%3DBE%3C%2Fissuer%3E%3Cserial_number%3E1208925819
615913170207512%3C%2Fserial_number%3E%3Csignature_algorithm%3ESHA1withRSA%3C%2Fsignature_a
lgorithm%3E%3Cfrom_date%3EWed+Sep+08+17%3A27%3A26+PDT+2010%3C%2Ffrom_date%3E%3Cto_dat
e%3EFri+Sep+09+17%3A27%3A23+PDT+2011%3C%2Fto_date%3E%3Cversion%3E2%3C%2Fversion%3E%
3Cpublic_key%3ESun+RSA+public+key%2C+2048+bits%3C%2Fpublic_key%3E%3C%2Fcertificate%3E%3Cce
rtificate+expired%3D%22false%22%3E%3Csubject%3ECN%3DGlobalSign+Domain+Validation+CA%2C+O%3
DGlobalSign+nv-
sa%2C+OU%3DDomain+Validation+CA%2C+C%3DBE%3C%2Fsubject%3E%3Cissuer%3ECN%3DGlobalSign
+Root+CA%2C+OU%3DRoot+CA%2C+O%3DGlobalSign+nv-
sa%2C+C%3DBE%3C%2Fissuer%3E%3Cserial_number%3E48357032784597462111995 32%3C%2Fserial_nu
mber%3E%3Csignature_algorithm%3ESHA1withRSA%3C%2Fsignature_algorithm%3E%3Cfrom_date%3EFri+
May+04+03%3A00%3A00+PDT+2007%3C%2Ffrom_date%3E%3Cto_date%3EThu+May+04+05%3A00%3A00
+PDT+2017%3C%2Fto_date%3E%3Cversion%3E2%3C%2Fversion%3E%3Cpublic_key%3ESun+RSA+public+
key%2C+2048+bits%3C%2Fpublic_key%3E%3C%2Fcertificate%3E%3Cssl_cert_mismatch%3Efalse%3C%2Fs
sl_cert_mismatch%3E%3Cssl_cert_self_signed%3Efalse%3C%2Fssl_cert_self_signed%3E%3Cnegotiated_prot
ocol%3ETLSv1%3C%2Fnegotiated_protocol%3E%3Cnegotiated_cipher%3ETLS_RSA_WITH_AES_128_CBC_
SHA%3C%2Fnegotiated_cipher%3E%3Cserver_enabled_cipher%3ETLS_RSA_WITH_AES_128_CBC_SHA%3
C%2Fserver_enabled_cipher%3E%3C%2Fsslreport%3E

Links

None

References

None

Severity	Name	Port	Category	Status
1	Missing Secure Attribute in an Encrypted Session (SSL) Cookie	443/tcp	Web Application	Pass

Description

The application sets a cookie over a secure channel without using the "secure" attribute. RFC states that if the cookie does not have the secure attribute assigned to it, then the cookie can be passed to the server by the client over non-secure channels (http). Using this attack, an attacker may be able to intercept this cookie, over the non-secure channel, and use it for a session hijacking attack.

CVSS Score

2.1

CVSS Fingerprint

AV:L/AC:L/Au:N/C:P/I:N/A:N

Solution

It is best business practice that any cookies that are sent (set-cookie) over an SSL connection to explicitly state secure on them.

Details

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							

Path: / --> No "Secure" Attribute on Secure Channel (https) : ASP.NET_SessionId=2fxfcs45woviqrqg44lndo3x; path=/; HttpOnly

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							

Path: / --> No "Secure" Attribute on Secure Channel (https) : ASP.NET_SessionId=34guskacge0yrqzp3jkjng55; path=/; HttpOnly

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/erpoiuh2vi4r23E2f.html							
Headers	Host=83.231.190.50 TRACKTRACE=%3Chtml%3E%3Cbody%3EMcafeeSecure%2FTRACKTRACE+%3Cscript%3Ealert%28%27TRACK%2FTRACE%27%29%3C%2Fscript%3E%3C%2Fbody%3E%3C%2Fhtml%3E Cookie=							

Path: /erpoiuh2vi4r23E2f.html --> No "Secure" Attribute on Secure Channel (https) : ASP.NET_SessionId=zh2p0z45qxfzyhrljd14ryep; path=/; HttpOnly

Links

owasp
RFC 2109 - HTTP State Management Mechanism
Persistent Client State HTTP Cookies

References

CVE CVE-2004-0462
Open Source Vulnerability Database 19183

Severity	Name	Port	Category	Status
1	Potentially Sensitive Information Missing Secure Attribute in an Encrypted Session (SSL) Cookie	443/tcp	Web Application	Pass

Description

The application sets a cookie over a secure channel without using the "secure" attribute. RFC states that if the cookie does not have the secure attribute assigned to it, then the cookie can be passed to the server by the client over non-secure channels (http). Using this attack, an attacker may be able to intercept this cookie, over the non-secure channel, and use it for a session hijacking attack.

The information that was sent was flagged as being potentially sensitive. Potentially sensitive information could be session tokens, user id's, or passwords.

CVSS Score

2.1

CVSS Fingerprint

AV:L/AC:L/Au:N/C:P/I:N/A:N

Solution

It is best business practice that any cookies that are sent (set-cookie) over an SSL connection to explicitly state secure on them. Speak with your web developer to have them enable the secure attribute on cookies sent over secure connections.

Details

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							

Path: / --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=2fxfcs45woviqrqg44lndo3x; path=/; HttpOnly

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							

Path: / --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=34guskacge0yrqzp3jkjng55; path=/; HttpOnly

Protocol	https	**Port**	443	**Read Timeout**	10000	**Method**	GET	Demo

Path	/erpoiuh2vi4r23E2f.html
Headers	Host=83.231.190.50 TRACKTRACE=%3Chtml%3E%3Cbody%3EMcafeeSecure%2FTRACKTRACE+%3Cscript%3Ealert%28%27TRACK%2FTRACE%27%29%3C%2Fscript%3E%3C%2Fbody%3E%3C%2Fhtml%3E Cookie=

Path: /erpoiuh2vi4r23E2f.html --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=zh2p0z45qxfzyhrljd14ryep; path=/; HttpOnly

Links

CWE.Mitre.org
Persistent Client State HTTP Cookies
CVE..Mitre.org
RFC 2109 - HTTP State Management Mechanism

References

CVE CVE-2004-0462

Severity	Name	Port	Category	Status
1	Potentially Sensitive Information Missing Secure Attribute in an Encrypted Session (SSL) Cookie	80/tcp	Web Application	Pass

Description

The application sets a cookie over a secure channel without using the "secure" attribute. RFC states that if the cookie does not have the secure attribute assigned to it, then the cookie can be passed to the server by the client over non-secure channels (http). Using this attack, an attacker may be able to intercept this cookie, over the non-secure channel, and use it for a session hijacking attack.

The information that was sent was flagged as being potentially sensitive. Potentially sensitive information could be session tokens, user id's, or passwords.

CVSS Score

2.1

CVSS Fingerprint

AV:L/AC:L/Au:N/C:P/I:N/A:N

Solution

It is best business practice that any cookies that are sent (set-cookie) over an SSL connection to explicitly state secure on them. Speak with your web developer to have them enable the secure attribute on cookies sent over secure connections.

Details

Protocol	http	**Port**	80	**Read Timeout**	10000	**Method**	GET	Demo
Path	/							

Path: / --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=ll2vmq313qjdf3zdrf4xedu5; path=/; HttpOnly

Protocol	http	**Port**	80	**Read Timeout**	10000	**Method**	GET	Demo
Path	/							

Path: / --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=1jufcm55jsutswbg2xxjzcvk; path=/; HttpOnly

Protocol	http	**Port**	80	**Read Timeout**	10000	**Method**	GET	Demo
Path	/							

Path: / --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=pug030jfpe1oq0untkdowv55; path=/; HttpOnly

Protocol	http	Port	80	Read Timeout	90000	Method	GET	Demo
Path	/BACLIENT							

Path: /BACLIENT --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=31guztytnj1say55cq4siw45; path=/; HttpOnly

Links

CWE.Mitre.org
Persistent Client State HTTP Cookies
CVE..Mitre.org
RFC 2109 - HTTP State Management Mechanism

References

CVE CVE-2004-0462

3.2.5 - Resolved: 83.231.190.50

None

3.3.1 - Overview: 192.150.2.140 / nj.worldsecuresystems.com (192.150.2.140)

Scan Date	1	2	3	4	5
03-DEC-2010 22:31	13	1	0	0	0

3.3.2 - Open Ports: 192.150.2.140 / nj.worldsecuresystems.com (192.150.2.140)

Port	Protocol	Service	Banner
21	tcp	ftp	ftp
80	tcp	http	http
443	tcp	https	https

3.3.3 - Consolidated Solution: 192.150.2.140 / nj.worldsecuresystems.com (192.150.2.140)

All level 3, 4, and 5 vulnerabilities identified for this device must be addressed with mitigation or remediation in order to satisfy PCI requirements.
Review all findings for this device, then for each vulnerability with level 3, 4, or 5, implement the solution described or an equivalent solution. Regenerate and submit the report based on scan results taken after remediation is completed.
If mitigations are employed according to the compensating controls mechanism of PCI, you must provide details of compensating controls for each level 3, 4, or 5 vulnerability that appears in this report.

3.3.4 - Vulnerabilities: 192.150.2.140 / nj.worldsecuresystems.com (192.150.2.140)

Severity	Name	Port	Category	Status
2	Unencrypted Sensitive Form Detected	80/tcp	Web Application	Pass

Description

The remote host appears to allow sensitive form submission over unencrypted (HTTP) connections. This means that a user's personal information is sent over the internet in clear text. An attacker may be able to uncover sensitive information such as login names and passwords by sniffing network traffic. All web pages that transmit Card Holder Data or Personally Identifiable Information (PII)**. Examples: - Users and/or Administrators login to the web site. - Registration forms such as user signup pages. - Updating User and/or Administrators profile pages. - Updating User and/or Administrators shipping information pages. - Forgot password reset page. - Company "Contact Us" pages.

** These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI DSS requirements for general protection of the cardholder data environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

CVSS Score

5.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:P

Solution

Plain-text protocols should never by used to transmit sensitive information over the Internet. When passing sensitive information to the web server, use HTTPS (SSLv3, TLS 1) instead of HTTP.

Details

Protocol	http	**Port**	80	**Read Timeout**	10000	**Method**	POST	Demo
Path	/ZoneProcess.aspx							
Query	ZoneID=-1 OID=7 OTYPE=1							
Headers	Referer=http%3A%2F%2F192.150.2.140%2FMembersOnly.htm							

	Content-Type=application%2Fx-www-form-urlencoded
Body	Username= Password=p455w0rd

Protocol	http	**Port**	80	**Read Timeout**	10000	**Method**	POST	Demo

Path	/ZoneProcess.aspx
Query	ZoneID=-1 OID=7 OTYPE=1
Headers	Referer=http%3A%2F%2F192.150.2.140%2FMembersOnly.htm Content-Type=application%2Fx-www-form-urlencoded
Body	Username= Password=

Form on page: /MembersOnly.htm

Links

Information on ARP poisoning
Information on man-in-the-middle attacks
Example software used to audit man-in-the-middle vulnerabilities

References

None

Severity	Name	Port	Category	Status
1	SSL Cert Mismatch	443/tcp	Web Server	Pass

Description

The SSL certificate does NOT match the website. This may prevent users from trusting/validating the website or service.
Example, if the SSL certificate has been issued for [www.paypal.com] and the site is accessed via [paypal.com]; the user will receive the following security warning.

"The security certificate presented by this website was issued for a different website's address."

CVSS Score

0.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution

Contact the web administrator to correct/create a new SSL certificate using the correct website name.

Details

Subject(s) on cert do(es) not match target host { Target Host : SubjectCN(s) }. {192.150.2.140 : *.worldsecuresystems.com}

Links

SSL Certificates - Security Certificate Errors

References

None

Severity	Name	Port	Category	Status
1	SSL Cert Info	443/tcp	Web Server	Pass

Description

This test attempts to provide details pertaining to your SSL certificate.

CVSS Score

0.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution

None

Details

%3C%3Fxml+version%3D%221.0%22+encoding%3D%22UTF-
8%22+standalone%3D%22no%22%3F%3E%3Csslreport%3E%3Ccertificate+expired%3D%22false%22%3E%3
Csubject%3ECN%3D*.worldsecuresystems.com%2C+O%3D*.worldsecuresystems.com%2C+OU%3DDomain+
Control+Validated%2C+C%3DUS%3C%2Fsubject%3E%3Cissuer%3ECN%3DGlobalSign+Domain+Validation+
CA%2C+O%3DGlobalSign+nv-
sa%2C+OU%3DDomain+Validation+CA%2C+C%3DBE%3C%2Fissuer%3E%3Cserial_number%3E1208925819
615913170207512%3C%2Fserial_number%3E%3Csignature_algorithm%3ESHA1withRSA%3C%2Fsignature_a
lgorithm%3E%3Cfrom_date%3EWed+Sep+08+17%3A27%3A26+PDT+2010%3C%2Ffrom_date%3E%3Cto_dat
e%3EFri+Sep+09+17%3A27%3A23+PDT+2011%3C%2Fto_date%3E%3Cversion%3E2%3C%2Fversion%3E%
3Cpublic_key%3ESun+RSA+public+key%2C+2048+bits%3C%2Fpublic_key%3E%3C%2Fcertificate%3E%3Cce
rtificate+expired%3D%22false%22%3E%3Csubject%3ECN%3DGlobalSign+Domain+Validation+CA%2C+O%3
DGlobalSign+nv-
sa%2C+OU%3DDomain+Validation+CA%2C+C%3DBE%3C%2Fsubject%3E%3Cissuer%3ECN%3DGlobalSign
+Root+CA%2C+OU%3DRoot+CA%2C+O%3DGlobalSign+nv-
sa%2C+C%3DBE%3C%2Fissuer%3E%3Cserial_number%3E48357032784597462111991 25%3C%2Fserial_nu
mber%3E%3Csignature_algorithm%3ESHA1withRSA%3C%2Fsignature_algorithm%3E%3Cfrom_date%3EFri+
May+04+03%3A00%3A00+PDT+2007%3C%2Ffrom_date%3E%3Cto_date%3EThu+May+04+05%3A00%3A00
+PDT+2017%3C%2Fto_date%3E%3Cversion%3E2%3C%2Fversion%3E%3Cpublic_key%3ESun+RSA+public+
key%2C+2048+bits%3C%2Fpublic_key%3E%3C%2Fcertificate%3E%3Cssl_cert_mismatch%3Efalse%3C%2Fs
sl_cert_mismatch%3E%3Cssl_cert_self_signed%3Efalse%3C%2Fssl_cert_self_signed%3E%3Cnegotiated_prot
ocol%3ETLSv1%3C%2Fnegotiated_protocol%3E%3Cnegotiated_cipher%3ESSL_RSA_WITH_RC4_128_MD5
%3C%2Fnegotiated_cipher%3E%3Cserver_enabled_cipher%3ESSL_RSA_WITH_RC4_128_MD5%3C%2Fserv
er_enabled_cipher%3E%3C%2Fsslreport%3E

Links

None

References

None

Severity	Name	Port	Category	Status
1	AutoComplete attribute is true	443/tcp	Information Gathering	Pass

Description

The remote web server contains form fields that allow for auto completion. Depending on the values entered into these fields, future users could obtain sensitive information previously entered by past users.

Fields that contain sensitive information, such as credit card and social security numbers and passwords, must be disallowed from caching information.

CVSS Score

2.6

CVSS Fingerprint

AV:N/AC:H/Au:N/C:P/I:N/A:N

Solution

To disable all entries in a form from being cached, the autocomplete value of the form tag must be set to "off", such as:

<form method="POST" action="handlepayment.asp" autocomplete="off">

The autocomplete attribute can also be used on an individual form element such as:

<input type="password" autocomplete="off" name="password">

Details

Protocol	https	**Port**	443	**Read Timeout**	10000	**Method**	GET	Demo
Path	/MembersOnly.htm							
Headers	Host=192.150.2.140 Referer=https%3A%2F%2F192.150.2.140%2Fphplive%2Findex.php							

Protocol	https	**Port**	443	**Read Timeout**	10000	**Method**	POST	Demo
Path	/ZoneProcess.aspx							
Query	ZoneID=-1 OID=7 OTYPE=1							
Headers	Referer=https%3A%2F%2F192.150.2.140%2FMembersOnly.htm Content-Type=application%2Fx-www-form-urlencoded							
Body	Username= Password=							

Form on page: /MembersOnly.htm

Links

None

References

None

Severity	Name	Port	Category	Status
1	Missing Secure Attribute in an Encrypted Session (SSL) Cookie	443/tcp	Web Application	Pass

Description

The application sets a cookie over a secure channel without using the "secure" attribute. RFC states that if the cookie does not have the secure attribute assigned to it, then the cookie can be passed to the server by the client over non-secure channels (http). Using this attack, an attacker may be able to intercept this cookie, over the non-secure channel, and use it for a session hijacking attack.

CVSS Score

2.1

CVSS Fingerprint

AV:L/AC:L/Au:N/C:P/I:N/A:N

Solution

It is best business practice that any cookies that are sent (set-cookie) over an SSL connection to explicitly state secure on them.

Details

Protocol	https	**Port**	443	**Read Timeout**	10000	**Method**	GET	Demo
Path	/							

Path: / --> No "Secure" Attribute on Secure Channel (https) : ANONID75144=c60e3704-892d-4941-be10-0f28b9eda31a; domain=192.150.2.140; expires=Sun, 04-Dec-2011 06:20:24 GMT; path=/

Protocol	https	**Port**	443	**Read Timeout**	10000	**Method**	GET	Demo
Path	/							

Path: / --> No "Secure" Attribute on Secure Channel (https) : VISID75144=223506c2-2fdc-431b-80e3-58e7df9de92e; domain=192.150.2.140; expires=Sat, 04-Dec-2010 07:20:24 GMT; path=/

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							
Headers	User-Agent=Mozilla%2F5.0+%28compatible%3B+MSIE+7.0%3B+MSIE+6.0%3B+DoCoMo%3B+Nokia%3B+SymbianOS%3B+NetFront%3B+XENIUM%3B+PPC%3B+ScanAlert%3B+%2Bhttp%3A%2F%2Fwww.mcafeesecure.com%2Fbot.jsp+%29							

Path: / --> No "Secure" Attribute on Secure Channel (https) : ANONID75144=c60e3704-892d-4941-be10-0f28b9eda31a; domain=192.150.2.140; expires=Sun, 04-Dec-2011 06:22:00 GMT; path=/

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							
Headers	User-Agent=Mozilla%2F5.0+%28compatible%3B+MSIE+7.0%3B+MSIE+6.0%3B+DoCoMo%3B+Nokia%3B+SymbianOS%3B+NetFront%3B+XENIUM%3B+PPC%3B+ScanAlert%3B+%2Bhttp%3A%2F%2Fwww.mcafeesecure.com%2Fbot.jsp+%29							

Path: / --> No "Secure" Attribute on Secure Channel (https) : VISID75144=223506c2-2fdc-431b-80e3-58e7df9de92e; domain=192.150.2.140; expires=Sat, 04-Dec-2010 07:22:00 GMT; path=/

Protocol	https	Port	443	Read Timeout	10000	Method	OPTIONS	Demo
Path	/							

Path: / --> No "Secure" Attribute on Secure Channel (https) : ANONID75144=c60e3704-892d-4941-be10-0f28b9eda31a; domain=192.150.2.140; expires=Sun, 04-Dec-2011 06:25:34 GMT; path=/

Protocol	https	Port	443	Read Timeout	10000	Method	OPTIONS	Demo
Path	/							

Path: / --> No "Secure" Attribute on Secure Channel (https) : VISID75144=223506c2-2fdc-431b-80e3-58e7df9de92e; domain=192.150.2.140; expires=Sat, 04-Dec-2010 07:25:34 GMT; path=/

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							

Path: / --> No "Secure" Attribute on Secure Channel (https) : ASP.NET_SessionId=z0yqdanscake1x55k2recp2i; path=/; HttpOnly

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							

Path: / --> No "Secure" Attribute on Secure Channel (https) : ASP.NET_SessionId=noiyal45uzei3555iegbvimn; path=/; HttpOnly

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							
Headers	Expect=%3Cscript%3Ealert%288888%29%3C%2Fscript%3E							

Path: / --> No "Secure" Attribute on Secure Channel (https) : ANONID75144=c60e3704-892d-4941-be10-0f28b9eda31a; domain=192.150.2.140; expires=Sun, 04-Dec-2011 06:26:34 GMT; path=/

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							
Headers	Expect=%3Cscript%3Ealert%288888%29%3C%2Fscript%3E							

Path: / --> No "Secure" Attribute on Secure Channel (https) : VISID75144=223506c2-2fdc-431b-80e3-58e7df9de92e; domain=192.150.2.140; expires=Sat, 04-Dec-2010 07:26:34 GMT; path=/

Links

owasp
RFC 2109 - HTTP State Management Mechanism
Persistent Client State HTTP Cookies

References

CVE CVE-2004-0462
Open Source Vulnerability Database 19183

Severity	Name	Port	Category	Status
1	Potentially Sensitive Information Missing Secure Attribute in an Encrypted Session (SSL) Cookie	443/tcp	Web Application	Pass

Description

The application sets a cookie over a secure channel without using the "secure" attribute. RFC states that if the cookie does not have the secure attribute assigned to it, then the cookie can be passed to the server by the client over non-secure channels (http). Using this attack, an attacker may be able to intercept this cookie, over the non-secure channel, and use it for a session hijacking attack.

The information that was sent was flagged as being potentially sensitive. Potentially sensitive information could be session tokens, user id's, or passwords.

CVSS Score

2.1

CVSS Fingerprint

AV:L/AC:L/Au:N/C:P/I:N/A:N

Solution

It is best business practice that any cookies that are sent (set-cookie) over an SSL connection to explicitly state secure on them. Speak with your web developer to have them enable the secure attribute on cookies sent over secure connections.

Details

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							

Path: / --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=z0yqdanscake1x55k2recp2i; path=/; HttpOnly

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							

Path: / --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=noiyal45uzei3555iegbvimn; path=/; HttpOnly

Links

CWE.Mitre.org
Persistent Client State HTTP Cookies
CVE..Mitre.org
RFC 2109 - HTTP State Management Mechanism

References

CVE CVE-2004-0462

Severity	Name	Port	Category	Status
1	SSL Cipher Suites Supported	443/tcp	Web Application	Pass

Description

This script detects which SSL ciphers are supported by the remote service for encrypting communications.

CVSS Score

2.6

CVSS Fingerprint

AV:N/AC:H/Au:N/C:P/I:N/A:N

Solution

Ensure that your server is capable of supporting the latest and strongest strength ciphers. Keeping your server patched and updated is helpful.

For more information view the openssl link below.

Details

Here is the list of SSL ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)
SSLv3
EDH-RSA-DES-CBC3-SHA Kx=DH Au=RSA Enc=3DES(168) Mac=SHA1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

Links

www.openssl.org/docs/apps/ciphers.html

References

None

Severity	Name	Port	Category	Status
1	SSL Certificate Information	443/tcp	Web Server	Pass

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

CVSS Score

0.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution

Please disable if you have any low strength ciphers

Details

Subject Name:

Country: US
Organization Unit: Domain Control Validated
Organization: *.worldsecuresystems.com
Common Name: *.worldsecuresystems.com

Issuer Name:

Country: BE
Organization Unit: Domain Validation CA
Organization: GlobalSign nv-sa
Common Name: GlobalSign Domain Validation CA

Serial Number: 01 00 00 00 00 01 2A F4 18 83 18

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Sep 09 00:27:26 2010 GMT
Not Valid After: Sep 10 00:27:23 2011 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 C5 EE 8B C9 C9 A2 62 E5 74 A4 DE FD 6B 63 C6 24 8F A0 7A
EC A0 6F BD 13 DB 5D 1C 66 53 A7 CF DF 4B 40 02 93 6B B2 04
CB 30 E6 0A F6 44 F1 96 C8 8B E0 CE DD 64 F8 D3 B1 1C 1F F4
08 50 A3 F3 73 03 DE 5C 7F 40 77 55 73 72 A8 79 48 9D 22 F9
24 D6 F4 CD DA 60 3D E3 3E 4D 99 24 2E B9 76 D9 EC 8B 80 54
6C 47 E2 60 13 F6 C7 E7 D3 F1 89 F5 DA B1 A0 E4 05 CC 21 7F
53 80 EA 0C 47 20 61 41 6E AB FF E7 D5 47 0F 5C 98 93 27 C7
70 38 39 A2 42 A4 BE 83 0E F6 3C 7D B0 05 1C F3 5D 53 65 90
51 41 EC 51 68 37 F2 4F 4D 79 A3 BE AC 55 00 4A 81 EC 14 C0
F6 E8 6B 80 98 2B E5 BC 2D 25 14 EE 06 D5 21 E0 C0 0F C0 E4
56 6A AF 87 E0 D1 7D B2 11 D9 79 70 48 55 BA 03 D4 18 D0 1A
DD C5 8C FF 5C 6C D2 F5 2C 98 19 5B C9 F4 65 DC 98 FB 24 D2
36 8D F9 E6 42 B5 3E 23 C7 82 16 FC 5B B5 91 75 FF
Exponent: 01 00 01

Signature: 00 0F DD 5D 8A 26 D7 F3 EE DC C8 86 EF D7 D1 23 A6 C7 E6 F2
29 45 EC B2 F9 F0 DE 4E A1 F4 D4 33 DB EB 3C EA A1 3D D2 76
E5 EB EA 93 3B E4 0B 1A 7F B9 45 F8 FF 4D C9 E0 F5 9E 30 F6
7C 65 A1 AD 80 ED 60 1F EB A7 96 EB 1E D1 77 E8 31 3A 44 1B
42 86 62 60 F5 83 11 09 A7 C1 DB 90 29 B9 04 D6 88 66 7F 65
13 CE 16 E4 56 50 3D CE D9 3C D7 FD 2D 81 F0 74 03 65 35 4F
E6 C4 7D 38 E9 E4 C4 AA 50 A3 34 B9 2B F6 FA 3E 87 9C E8 F6
B4 40 8D 62 2C F6 A6 B1 1F 9E FB 4D 35 3F CB 6B 17 9F E4 25
DE 10 3B 6B C6 1A F0 DE A3 34 0E 1D EB A1 B4 8F 79 4C 2C BC
D9 14 00 B2 B5 55 ED 4B A1 84 39 6B A9 74 CD 4C 7B E1 31 D3
D0 1C 62 E8 92 CA 29 2F 05 AE 06 8C A2 99 2F 17 F3 3C 53 E1
5A 89 01 4E F1 D2 14 58 3C 42 55 78 93 67 A3 78 34 7F 80 18
BE 41 69 F7 5C 73 A0 16 E7 4E 84 5C 39 0B 24 2E 3F

Extension: Authority Key Identifier (2.5.29.35)
Critical: 0

Extension: Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical: 0
Method#1: Certificate Authority Issuers
URI: http://secure.globalsign.net/cacert/dvhe1.crt

Extension: CRL Distribution Points (2.5.29.31)
Critical: 0
URI: http://crl.globalsign.net/DomainVal1.crl

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: CB 94 6E A1 E6 3D 08 F7 B9 4B 04 0B 53 B6 25 B4 F7 BF 15 C3

Extension: Basic Constraints (2.5.29.19)
Critical: 0
Data: 30 00

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment

Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2)
Purpose#3: Microsoft Server Gated Crypto (SGC) (1.3.6.1.4.1.311.10.3.3)

Extension: Policies (2.5.29.32)
Critical: 0
Policy ID #1: 1.3.6.1.4.1.4146.1.10
Qualifier ID #1: Certification Practice Statement (1.3.6.1.5.5.7.2.1)
CPS URI: http://www.globalsign.net/repository/

Extension: 2.16.840.1.113730.1.1
Critical: 0
Data: 03 02 06 C0

Extension: Subject Alternative Name (2.5.29.17)
Critical: 0
DNS: *.worldsecuresystems.com
DNS: worldsecuresystems.com

Links

Transport Layer Security
SSL 2.0
IBM HTTP Server
Disabling SSLv2 in IIS (English)
Mozillazine

References

None

Severity	Name	Port	Category	Status
1	AutoComplete attribute is true	80/tcp	Information Gathering	Pass

Description

The remote web server contains form fields that allow for auto completion. Depending on the values entered into these fields, future users could obtain sensitive information previously entered by past users.

Fields that contain sensitive information, such as credit card and social security numbers and passwords, must be disallowed from caching information.

CVSS Score

2.6

CVSS Fingerprint

AV:N/AC:H/Au:N/C:P/I:N/A:N

Solution

To disable all entries in a form from being cached, the autocomplete value of the form tag must be set to "off", such as:

<form method="POST" action="handlepayment.asp" autocomplete="off">

The autocomplete attribute can also be used on an individual form element such as:

<input type="password" autocomplete="off" name="password">

Details

Protocol	http	Port	80	Read Timeout	10000	Method	GET	Demo
Path	/MembersOnly.htm							
Headers	Host=192.150.2.140 Referer=http%3A%2F%2F192.150.2.140%2Fphplive%2Findex.php							

Protocol	http	Port	80	Read Timeout	10000	Method	POST	Demo
Path	/ZoneProcess.aspx							
Query	ZoneID=-1 OID=7 OTYPE=1							
Headers	Referer=http%3A%2F%2F192.150.2.140%2FMembersOnly.htm Content-Type=application%2Fx-www-form-urlencoded							
Body	Username= Password=							

Form on page: /MembersOnly.htm

Links

None

References

None

Severity	Name	Port	Category	Status
1	Potentially Sensitive Information Missing Secure Attribute in an Encrypted Session (SSL) Cookie	80/tcp	Web Application	Pass

Description

The application sets a cookie over a secure channel without using the "secure" attribute. RFC states that if the cookie does not have the secure attribute assigned to it, then the cookie can be passed to the server by the client over non-secure channels (http). Using this attack, an attacker may be able to intercept this cookie, over the non-secure channel, and use it for a session hijacking attack.

The information that was sent was flagged as being potentially sensitive. Potentially sensitive information could be session tokens, user id's, or passwords.

CVSS Score

2.1

CVSS Fingerprint

AV:L/AC:L/Au:N/C:P/I:N/A:N

Solution

It is best business practice that any cookies that are sent (set-cookie) over an SSL connection to explicitly state secure on them. Speak with your web developer to have them enable the secure attribute on cookies sent over secure connections.

Details

Protocol	http	**Port**	80	**Read Timeout**	10000	**Method**	GET	Demo
Path	/							

Path: / --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=4243ec45kpodrj55n1xyxqru; path=/; HttpOnly

Protocol	http	**Port**	80	**Read Timeout**	90000	**Method**	GET	Demo
Path	/BACLIENT							

Path: /BACLIENT --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=44rvip45cozpap451ldgo155; path=/; HttpOnly

Protocol	http	**Port**	80	**Read Timeout**	10000	**Method**	GET	Demo
Path	/							

Path: / --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=00aw1hz1i4hmdcynwrnnfqq1; path=/; HttpOnly

Protocol	http	**Port**	80	**Read Timeout**	10000	**Method**	GET	Demo
Path	/							

Path: / --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=h3z1qj55s30zy3z31wzu5x45; path=/; HttpOnly

Links

CWE.Mitre.org
Persistent Client State HTTP Cookies
CVE..Mitre.org
RFC 2109 - HTTP State Management Mechanism

References

CVE CVE-2004-0462

Severity	Name	Port	Category	Status
1	FTP Supports Clear Text Authentication	21/tcp	FTP	Pass

Description

The remote FTP server allows the user's name and password to be transmitted in clear text, which may be intercepted by a network sniffer, or a man-in-the-middle attack.

CVSS Score

2.6

CVSS Fingerprint

AV:N/AC:H/Au:N/C:P/I:N/A:N

Solution

Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server such that control connections are encrypted.

Details

:

This FTP server does not support 'AUTH TLS'.
Other references : CWE:522, CWE:523

Links

Configuring & Using SSH/SFTP
Configuring vsftpd for Secure Connections
Setting up ProFTPd & TLS on Debian Etch
Filezilla - Free (GPL) FTP(S) & SFTP Client (Windows, Linux, OS X)

References

None

Severity	Name	Port	Category	Status
1	FTP Server Detection	21/tcp	FTP	Pass

Description

It is possible to obtain the banner of the remote FTP server by connecting to the remote port.

CVSS Score

0.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution

N/A

Details

The remote FTP banner is :

220-**********

220-Welcome to FTP

220-Please use your email address and password to login.

220-If you are registered for more than one site then your login name must be:
yourcompany.com/you@youremail.com.

220-**********

220-

220 FTP Server Ready

Links

None

References

None

Severity	Name	Port	Category	Status
1	TCP Timestamps	All	Other	Pass

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

CVSS Score

0.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution

n/a

Details

Synopsis :

The remote service implements TCP timestamps.

Description :

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See also :

http://www.ietf.org/rfc/rfc1323.txt

Solution :

n/a

Risk factor :

None

Links

www.ietf.org/rfc/rfc1323.txt

References

None

Severity	Name	Port	Category	Status
1	OS Identification	All	Other	Pass

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc...)
it is possible to guess the name of the remote operating system in use, and
sometimes its version

CVSS Score

0.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution

By modifying the banners of the services running and blocking ICMP requests at the firewall, OS fingerprinting can be limited.

Details

Synopsis :

It is possible to guess the remote operating system

Description :

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc...)
it is possible to guess the name of the remote operating system in use, and
sometimes its version

Solution :

N/A

Risk factor :

None

Plugin output :

Remote operating system : Microsoft Windows Server 2008
Confidence Level : 75
Method : HTTP

Not all fingerprints could give a match - please email the following to os-signatures@ScanAlert.org :
HTTP:Server: Microsoft-IIS/7.0
SinFP:!:
P1:B11113:F0x12:W1608:O0:M0:
P2:B11113:F0x12:W4380:O0204ffff010303010101080affffffff4445414404020000:M1460:
P3:B00000:F0x00:W0:O0:M0
P4:3209_7_p=443R
SSLcert:!:i/CN:GlobalSign Domain Validation CAi/O:GlobalSign nv-
sas/CN:*.worldsecuresystems.coms/O:*.worldsecuresystems.com

The remote host is running Microsoft Windows Server 2008

Links

None

References

None

3.3.5 - Resolved: 192.150.2.140 / nj.worldsecuresystems.com (192.150.2.140)

None

3.4.1 - Overview: 202.176.14.137 / syd.worldsecuresystems.com (202.176.14.137)

Scan Date	1	2	3	4	5
03-DEC-2010 22:34	13	1	0	0	0

3.4.2 - Open Ports: 202.176.14.137 / syd.worldsecuresystems.com (202.176.14.137)

Port	Protocol	Service	Banner
21	tcp	ftp	ftp
80	tcp	http	http
443	tcp	https	https

3.4.3 - Consolidated Solution: 202.176.14.137 / syd.worldsecuresystems.com (202.176.14.137)

All level 3, 4, and 5 vulnerabilities identified for this device must be addressed with mitigation or remediation in order to satisfy PCI requirements.
Review all findings for this device, then for each vulnerability with level 3, 4, or 5, implement the solution described or an equivalent solution. Regenerate and submit the report based on scan results taken after remediation is completed.
If mitigations are employed according to the compensating controls mechanism of PCI, you must provide details of compensating controls for each level 3, 4, or 5 vulnerability that appears in this report.

3.4.4 - Vulnerabilities: 202.176.14.137 / syd.worldsecuresystems.com (202.176.14.137)

Severity	Name	Port	Category	Status
2	Unencrypted Sensitive Form Detected	80/tcp	Web Application	Pass

Description

The remote host appears to allow sensitive form submission over unencrypted (HTTP) connections. This means that a user's personal information is sent over the internet in clear text. An attacker may be able to uncover sensitive information such as login names and passwords by sniffing network traffic. All web pages that transmit Card Holder Data or Personally Identifiable Information (PII)**. Examples: - Users and/or Administrators login to the web site. - Registration forms such as user signup pages. - Updating User and/or Administrators profile pages. - Updating User and/or Administrators shipping information pages. - Forgot password reset page. - Company "Contact Us" pages.

** These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI DSS requirements for general protection of the cardholder data environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

CVSS Score

5.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:P

Solution

Plain-text protocols should never by used to transmit sensitive information over the Internet. When passing sensitive information to the web server, use HTTPS (SSLv3, TLS 1) instead of HTTP.

Details

Protocol	http	**Port**	80	**Read Timeout**	10000	**Method**	POST	Demo
Path	/ZoneProcess.aspx							
Query	ZoneID=-1 OID=4518273 OTYPE=1							
Headers	Referer=http%3A%2F%2F202.176.14.137%2FMembersOnly.htm							

	Content-Type=application%2Fx-www-form-urlencoded
Body	Username= Password=p455w0rd

Protocol	http	**Port**	80	**Read Timeout**	10000	**Method**	POST	Demo
Path	/ZoneProcess.aspx							
Query	ZoneID=-1 OID=4518273 OTYPE=1							
Headers	Referer=http%3A%2F%2F202.176.14.137%2FMembersOnly.htm Content-Type=application%2Fx-www-form-urlencoded							
Body	Username= Password=							

Form on page: /MembersOnly.htm

Links

Information on ARP poisoning
Information on man-in-the-middle attacks
Example software used to audit man-in-the-middle vulnerabilities

References

None

Severity	Name	Port	Category	Status
1	SSL Cert Mismatch	443/tcp	Web Server	Pass

Description

The SSL certificate does NOT match the website. This may prevent users from trusting/validating the website or service.
Example, if the SSL certificate has been issued for [www.paypal.com] and the site is accessed via [paypal.com]; the user will receive the following security warning.

"The security certificate presented by this website was issued for a different website's address."

CVSS Score

0.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution

Contact the web administrator to correct/create a new SSL certificate using the correct website name.

Details

Subject(s) on cert do(es) not match target host { Target Host : SubjectCN(s) }. {202.176.14.137 : *.worldsecuresystems.com}

Links

SSL Certificates - Security Certificate Errors

References

None

Severity	Name	Port	Category	Status
1	SSL Cert Info	443/tcp	Web Server	Pass

Description

This test attempts to provide details pertaining to your SSL certificate.

CVSS Score

0.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution

None

Details

%3C%3Fxml+version%3D%221.0%22+encoding%3D%22UTF-
8%22+standalone%3D%22no%22%3F%3E%3Csslreport%3E%3Ccertificate+expired%3D%22false%22%3E%3
Csubject%3ECN%3D*.worldsecuresystems.com%2C+O%3D*.worldsecuresystems.com%2C+OU%3DDomain+
Control+Validated%2C+C%3DUS%3C%2Fsubject%3E%3Cissuer%3ECN%3DGlobalSign+Domain+Validation+
CA%2C+O%3DGlobalSign+nv-
sa%2C+OU%3DDomain+Validation+CA%2C+C%3DBE%3C%2Fissuer%3E%3Cserial_number%3E1208925819
615913170207512%3C%2Fserial_number%3E%3Csignature_algorithm%3ESHA1withRSA%3C%2Fsignature_a
lgorithm%3E%3Cfrom_date%3EWed+Sep+08+17%3A27%3A26+PDT+2010%3C%2Ffrom_date%3E%3Cto_dat
e%3EFri+Sep+09+17%3A27%3A23+PDT+2011%3C%2Fto_date%3E%3Cversion%3E2%3C%2Fversion%3E%
3Cpublic_key%3ESun+RSA+public+key%2C+2048+bits%3C%2Fpublic_key%3E%3C%2Fcertificate%3E%3Cce
rtificate+expired%3D%22false%22%3E%3Csubject%3ECN%3DGlobalSign+Domain+Validation+CA%2C+O%3
DGlobalSign+nv-
sa%2C+OU%3DDomain+Validation+CA%2C+C%3DBE%3C%2Fsubject%3E%3Cissuer%3ECN%3DGlobalSign
+Root+CA%2C+OU%3DRoot+CA%2C+O%3DGlobalSign+nv-
sa%2C+C%3DBE%3C%2Fissuer%3E%3Cserial_number%3E48357032784597462111991 25%3C%2Fserial_nu
mber%3E%3Csignature_algorithm%3ESHA1withRSA%3C%2Fsignature_algorithm%3E%3Cfrom_date%3EFri+
May+04+03%3A00%3A00+PDT+2007%3C%2Ffrom_date%3E%3Cto_date%3EThu+May+04+05%3A00%3A00
+PDT+2017%3C%2Fto_date%3E%3Cversion%3E2%3C%2Fversion%3E%3Cpublic_key%3ESun+RSA+public+
key%2C+2048+bits%3C%2Fpublic_key%3E%3C%2Fcertificate%3E%3Cssl_cert_mismatch%3Efalse%3C%2Fs
sl_cert_mismatch%3E%3Cssl_cert_self_signed%3Efalse%3C%2Fssl_cert_self_signed%3E%3Cnegotiated_prot
ocol%3ETLSv1%3C%2Fnegotiated_protocol%3E%3Cnegotiated_cipher%3ESSL_RSA_WITH_RC4_128_MD5
%3C%2Fnegotiated_cipher%3E%3Cserver_enabled_cipher%3ESSL_RSA_WITH_RC4_128_MD5%3C%2Fserv
er_enabled_cipher%3E%3C%2Fsslreport%3E

Links

None

References

None

Severity	Name	Port	Category	Status
1	AutoComplete attribute is true	443/tcp	Information Gathering	Pass

Description

The remote web server contains form fields that allow for auto completion. Depending on the values entered into these fields, future users could obtain sensitive information previously entered by past users.

Fields that contain sensitive information, such as credit card and social security numbers and passwords, must be disallowed from caching information.

CVSS Score

2.6

CVSS Fingerprint

AV:N/AC:H/Au:N/C:P/I:N/A:N

Solution

To disable all entries in a form from being cached, the autocomplete value of the form tag must be set to "off", such as:

<form method="POST" action="handlepayment.asp" autocomplete="off">

The autocomplete attribute can also be used on an individual form element such as:

<input type="password" autocomplete="off" name="password">

Details

Protocol	https	**Port**	443	**Read Timeout**	10000	**Method**	GET	Demo
Path	/MembersOnly.htm							
Headers	Host=202.176.14.137 Referer=https%3A%2F%2F202.176.14.137%2Fphplive%2Findex.php							

Protocol	https	**Port**	443	**Read Timeout**	10000	**Method**	POST	Demo
Path	/ZoneProcess.aspx							
Query	ZoneID=-1 OID=4518273 OTYPE=1							
Headers	Referer=https%3A%2F%2F202.176.14.137%2FMembersOnly.htm Content-Type=application%2Fx-www-form-urlencoded							
Body	Username= Password=							

Form on page: /MembersOnly.htm

Links

None

References

None

Severity	Name	Port	Category	Status
1	Missing Secure Attribute in an Encrypted Session (SSL) Cookie	443/tcp	Web Application	Pass

Description

The application sets a cookie over a secure channel without using the "secure" attribute. RFC states that if the cookie does not have the secure attribute assigned to it, then the cookie can be passed to the server by the client over non-secure channels (http). Using this attack, an attacker may be able to intercept this cookie, over the non-secure channel, and use it for a session hijacking attack.

CVSS Score

2.1

CVSS Fingerprint

AV:L/AC:L/Au:N/C:P/I:N/A:N

Solution

It is best business practice that any cookies that are sent (set-cookie) over an SSL connection to explicitly state secure on them.

Details

Protocol	https	**Port**	443	**Read Timeout**	10000	**Method**	GET	Demo
Path	/							

Path: / --> No "Secure" Attribute on Secure Channel (https) : ANONID108812=af14edd5-db68-4f1c-9308-4e1e07edf531; domain=202.176.14.137; expires=Sun, 04-Dec-2011 06:24:45 GMT; path=/

Protocol	https	**Port**	443	**Read Timeout**	10000	**Method**	GET	Demo
Path	/							

Path: / --> No "Secure" Attribute on Secure Channel (https) : VISID108812=224f341e-032e-4c24-9dcb-d5b8ee6b1a3e; domain=202.176.14.137; expires=Sat, 04-Dec-2010 07:24:45 GMT; path=/

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							
Headers	User-Agent=Mozilla%2F5.0+%28compatible%3B+MSIE+7.0%3B+MSIE+6.0%3B+DoCoMo%3B+Nokia%3B+SymbianOS%3B+NetFront%3B+XENIUM%3B+PPC%3B+ScanAlert%3B+%2Bhttp%3A%2F%2Fwww.mcafeesecure.com%2Fbot.jsp+%29							

Path: / --> No "Secure" Attribute on Secure Channel (https) : ANONID108812=af14edd5-db68-4f1c-9308-4e1e07edf531; domain=202.176.14.137; expires=Sun, 04-Dec-2011 06:26:11 GMT; path=/

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							
Headers	User-Agent=Mozilla%2F5.0+%28compatible%3B+MSIE+7.0%3B+MSIE+6.0%3B+DoCoMo%3B+Nokia%3B+SymbianOS%3B+NetFront%3B+XENIUM%3B+PPC%3B+ScanAlert%3B+%2Bhttp%3A%2F%2Fwww.mcafeesecure.com%2Fbot.jsp+%29							

Path: / --> No "Secure" Attribute on Secure Channel (https) : VISID108812=224f341e-032e-4c24-9dcb-d5b8ee6b1a3e; domain=202.176.14.137; expires=Sat, 04-Dec-2010 07:26:11 GMT; path=/

Protocol	https	Port	443	Read Timeout	10000	Method	OPTIONS	Demo
Path	/							

Path: / --> No "Secure" Attribute on Secure Channel (https) : ANONID108812=af14edd5-db68-4f1c-9308-4e1e07edf531; domain=202.176.14.137; expires=Sun, 04-Dec-2011 06:29:25 GMT; path=/

Protocol	https	Port	443	Read Timeout	10000	Method	OPTIONS	Demo
Path	/							

Path: / --> No "Secure" Attribute on Secure Channel (https) : VISID108812=224f341e-032e-4c24-9dcb-d5b8ee6b1a3e; domain=202.176.14.137; expires=Sat, 04-Dec-2010 07:29:25 GMT; path=/

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							

Path: / --> No "Secure" Attribute on Secure Channel (https) : ASP.NET_SessionId=rlm0hcjrxnnkrkr3022snuf2; path=/; HttpOnly

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							

Path: / --> No "Secure" Attribute on Secure Channel (https) : ASP.NET_SessionId=zpksddufusdx2c55mwy5nc45; path=/; HttpOnly

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							
Headers	Expect=%3Cscript%3Ealert%288888%29%3C%2Fscript%3E							

Path: / --> No "Secure" Attribute on Secure Channel (https) : ANONID108812=af14edd5-db68-4f1c-9308-4e1e07edf531; domain=202.176.14.137; expires=Sun, 04-Dec-2011 06:30:16 GMT; path=/

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							
Headers	Expect=%3Cscript%3Ealert%288888%29%3C%2Fscript%3E							

Path: / --> No "Secure" Attribute on Secure Channel (https) : VISID108812=224f341e-032e-4c24-9dcb-d5b8ee6b1a3e; domain=202.176.14.137; expires=Sat, 04-Dec-2010 07:30:16 GMT; path=/

Links

owasp
RFC 2109 - HTTP State Management Mechanism
Persistent Client State HTTP Cookies

References

CVE CVE-2004-0462
Open Source Vulnerability Database 19183

Severity	Name	Port	Category	Status
1	Potentially Sensitive Information Missing Secure Attribute in an Encrypted Session (SSL) Cookie	443/tcp	Web Application	Pass

Description

The application sets a cookie over a secure channel without using the "secure" attribute. RFC states that if the cookie does not have the secure attribute assigned to it, then the cookie can be passed to the server by the client over non-secure channels (http). Using this attack, an attacker may be able to intercept this cookie, over the non-secure channel, and use it for a session hijacking attack.

The information that was sent was flagged as being potentially sensitive. Potentially sensitive information could be session tokens, user id's, or passwords.

CVSS Score

2.1

CVSS Fingerprint

AV:L/AC:L/Au:N/C:P/I:N/A:N

Solution

It is best business practice that any cookies that are sent (set-cookie) over an SSL connection to explicitly state secure on them. Speak with your web developer to have them enable the secure attribute on cookies sent over secure connections.

Details

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							

Path: / --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=rlm0hcjrxnnkrkr3022snuf2; path=/; HttpOnly

Protocol	https	Port	443	Read Timeout	10000	Method	GET	Demo
Path	/							

Path: / --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=zpksddufusdx2c55mwy5nc45; path=/; HttpOnly

Links

CWE.Mitre.org
Persistent Client State HTTP Cookies
CVE..Mitre.org
RFC 2109 - HTTP State Management Mechanism

References

CVE CVE-2004-0462

Severity	Name	Port	Category	Status
1	SSL Cipher Suites Supported	443/tcp	Web Application	Pass

Description

This script detects which SSL ciphers are supported by the remote service for encrypting communications.

CVSS Score

2.6

CVSS Fingerprint

AV:N/AC:H/Au:N/C:P/I:N/A:N

Solution

Ensure that your server is capable of supporting the latest and strongest strength ciphers. Keeping your server patched and updated is helpful.

For more information view the openssl link below.

Details

Here is the list of SSL ciphers supported by the remote server :

High Strength Ciphers (>= 112-bit key)
SSLv3
EDH-RSA-DES-CBC3-SHA Kx=DH Au=RSA Enc=3DES(168) Mac=SHA1
DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

{OpenSSL ciphername}
Kx={key exchange}
Au={authentication}
Enc={symmetric encryption method}
Mac={message authentication code}
{export flag}

Links

www.openssl.org/docs/apps/ciphers.html

References

None

Severity	Name	Port	Category	Status
1	SSL Certificate Information	443/tcp	Web Server	Pass

Description

This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate.

CVSS Score

0.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution

Please disable if you have any low strength ciphers

Details

Subject Name:

Country: US
Organization Unit: Domain Control Validated
Organization: *.worldsecuresystems.com
Common Name: *.worldsecuresystems.com

Issuer Name:

Country: BE
Organization Unit: Domain Validation CA
Organization: GlobalSign nv-sa
Common Name: GlobalSign Domain Validation CA

Serial Number: 01 00 00 00 00 01 2A F4 18 83 18

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Sep 09 00:27:26 2010 GMT
Not Valid After: Sep 10 00:27:23 2011 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 C5 EE 8B C9 C9 A2 62 E5 74 A4 DE FD 6B 63 C6 24 8F A0 7A
EC A0 6F BD 13 DB 5D 1C 66 53 A7 CF DF 4B 40 02 93 6B B2 04
CB 30 E6 0A F6 44 F1 96 C8 8B E0 CE DD 64 F8 D3 B1 1C 1F F4
08 50 A3 F3 73 03 DE 5C 7F 40 77 55 73 72 A8 79 48 9D 22 F9
24 D6 F4 CD DA 60 3D E3 3E 4D 99 24 2E B9 76 D9 EC 8B 80 54
6C 47 E2 60 13 F6 C7 E7 D3 F1 89 F5 DA B1 A0 E4 05 CC 21 7F
53 80 EA 0C 47 20 61 41 6E AB FF E7 D5 47 0F 5C 98 93 27 C7
70 38 39 A2 42 A4 BE 83 0E F6 3C 7D B0 05 1C F3 5D 53 65 90
51 41 EC 51 68 37 F2 4F 4D 79 A3 BE AC 55 00 4A 81 EC 14 C0
F6 E8 6B 80 98 2B E5 BC 2D 25 14 EE 06 D5 21 E0 C0 0F C0 E4
56 6A AF 87 E0 D1 7D B2 11 D9 79 70 48 55 BA 03 D4 18 D0 1A
DD C5 8C FF 5C 6C D2 F5 2C 98 19 5B C9 F4 65 DC 98 FB 24 D2
36 8D F9 E6 42 B5 3E 23 C7 82 16 FC 5B B5 91 75 FF
Exponent: 01 00 01

Signature: 00 0F DD 5D 8A 26 D7 F3 EE DC C8 86 EF D7 D1 23 A6 C7 E6 F2
29 45 EC B2 F9 F0 DE 4E A1 F4 D4 33 DB EB 3C EA A1 3D D2 76
E5 EB EA 93 3B E4 0B 1A 7F B9 45 F8 FF 4D C9 E0 F5 9E 30 F6
7C 65 A1 AD 80 ED 60 1F EB A7 96 EB 1E D1 77 E8 31 3A 44 1B
42 86 62 60 F5 83 11 09 A7 C1 DB 90 29 B9 04 D6 88 66 7F 65
13 CE 16 E4 56 50 3D CE D9 3C D7 FD 2D 81 F0 74 03 65 35 4F
E6 C4 7D 38 E9 E4 C4 AA 50 A3 34 B9 2B F6 FA 3E 87 9C E8 F6
B4 40 8D 62 2C F6 A6 B1 1F 9E FB 4D 35 3F CB 6B 17 9F E4 25
DE 10 3B 6B C6 1A F0 DE A3 34 0E 1D EB A1 B4 8F 79 4C 2C BC
D9 14 00 B2 B5 55 ED 4B A1 84 39 6B A9 74 CD 4C 7B E1 31 D3
D0 1C 62 E8 92 CA 29 2F 05 AE 06 8C A2 99 2F 17 F3 3C 53 E1
5A 89 01 4E F1 D2 14 58 3C 42 55 78 93 67 A3 78 34 7F 80 18
BE 41 69 F7 5C 73 A0 16 E7 4E 84 5C 39 0B 24 2E 3F

Extension: Authority Key Identifier (2.5.29.35)
Critical: 0

Extension: Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical: 0
Method#1: Certificate Authority Issuers
URI: http://secure.globalsign.net/cacert/dvhe1.crt

Extension: CRL Distribution Points (2.5.29.31)
Critical: 0
URI: http://crl.globalsign.net/DomainVal1.crl

Extension: Subject Key Identifier (2.5.29.14)
Critical: 0
Subject Key Identifier: CB 94 6E A1 E6 3D 08 F7 B9 4B 04 0B 53 B6 25 B4 F7 BF 15 C3

Extension: Basic Constraints (2.5.29.19)
Critical: 0
Data: 30 00

Extension: Key Usage (2.5.29.15)
Critical: 1
Key Usage: Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment

Extension: Extended Key Usage (2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2)
Purpose#3: Microsoft Server Gated Crypto (SGC) (1.3.6.1.4.1.311.10.3.3)

Extension: Policies (2.5.29.32)
Critical: 0
Policy ID #1: 1.3.6.1.4.1.4146.1.10
Qualifier ID #1: Certification Practice Statement (1.3.6.1.5.5.7.2.1)
CPS URI: http://www.globalsign.net/repository/

Extension: 2.16.840.1.113730.1.1
Critical: 0
Data: 03 02 06 C0

Extension: Subject Alternative Name (2.5.29.17)
Critical: 0
DNS: *.worldsecuresystems.com
DNS: worldsecuresystems.com

Links

Transport Layer Security
SSL 2.0
IBM HTTP Server
Disabling SSLv2 in IIS (English)
Mozillazine

References

None

Severity	Name	Port	Category	Status
1	AutoComplete attribute is true	80/tcp	Information Gathering	Pass

Description

The remote web server contains form fields that allow for auto completion. Depending on the values entered into these fields, future users could obtain sensitive information previously entered by past users.

Fields that contain sensitive information, such as credit card and social security numbers and passwords, must be disallowed from caching information.

CVSS Score

2.6

CVSS Fingerprint

AV:N/AC:H/Au:N/C:P/I:N/A:N

Solution

To disable all entries in a form from being cached, the autocomplete value of the form tag must be set to "off", such as:

<form method="POST" action="handlepayment.asp" autocomplete="off">

The autocomplete attribute can also be used on an individual form element such as:

<input type="password" autocomplete="off" name="password">

Details

Protocol	http	**Port**	80	**Read Timeout**	10000	**Method**	GET	Demo
Path	/MembersOnly.htm							
Headers	Host=202.176.14.137 Referer=http%3A%2F%2F202.176.14.137%2Fphplive%2Findex.php							

Protocol	http	**Port**	80	**Read Timeout**	10000	**Method**	POST	Demo
Path	/ZoneProcess.aspx							
Query	ZoneID=-1 OID=4518273 OTYPE=1							
Headers	Referer=http%3A%2F%2F202.176.14.137%2FMembersOnly.htm Content-Type=application%2Fx-www-form-urlencoded							
Body	Username= Password=							

Form on page: /MembersOnly.htm

Links

None

References

None

Severity	Name	Port	Category	Status
1	Potentially Sensitive Information Missing Secure Attribute in an Encrypted Session (SSL) Cookie	80/tcp	Web Application	Pass

Description

The application sets a cookie over a secure channel without using the "secure" attribute. RFC states that if the cookie does not have the secure attribute assigned to it, then the cookie can be passed to the server by the client over non-secure channels (http). Using this attack, an attacker may be able to intercept this cookie, over the non-secure channel, and use it for a session hijacking attack.

The information that was sent was flagged as being potentially sensitive. Potentially sensitive information could be session tokens, user id's, or passwords.

CVSS Score

2.1

CVSS Fingerprint

AV:L/AC:L/Au:N/C:P/I:N/A:N

Solution

It is best business practice that any cookies that are sent (set-cookie) over an SSL connection to explicitly state secure on them. Speak with your web developer to have them enable the secure attribute on cookies sent over secure connections.

Details

Protocol	http	**Port**	80	**Read Timeout**	10000	**Method**	GET	Demo
Path	/							

Path: / --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=kvupldz3hflmys20ab2zbm45; path=/; HttpOnly

Protocol	http	**Port**	80	**Read Timeout**	90000	**Method**	GET	Demo
Path	/BACLIENT							

Path: /BACLIENT --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=ekjlmp45g2lb1l45tupktlr5; path=/; HttpOnly

Protocol	http	**Port**	80	**Read Timeout**	10000	**Method**	GET	Demo
Path	/							

Path: / --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=1cdcow45ieyxzyrckfdj3uz5; path=/; HttpOnly

Protocol	http	**Port**	80	**Read Timeout**	10000	**Method**	GET	Demo
Path	/							

Path: / --> Sensitive Info on secure Channel (https) without "Secure" Attribute : ASP.NET_SessionId=m53so0qoizvfhm55dh4np5vg; path=/; HttpOnly

Links

CWE.Mitre.org
Persistent Client State HTTP Cookies
CVE..Mitre.org
RFC 2109 - HTTP State Management Mechanism

References

CVE CVE-2004-0462

Severity	Name	Port	Category	Status
1	FTP Supports Clear Text Authentication	21/tcp	FTP	Pass

Description

The remote FTP server allows the user's name and password to be transmitted in clear text, which may be intercepted by a network sniffer, or a man-in-the-middle attack.

CVSS Score

2.6

CVSS Fingerprint

AV:N/AC:H/Au:N/C:P/I:N/A:N

Solution

Switch to SFTP (part of the SSH suite) or FTPS (FTP over SSL/TLS). In the latter case, configure the server such that control connections are encrypted.

Details

:

This FTP server does not support 'AUTH TLS'.
Other references : CWE:522, CWE:523

Links

Configuring & Using SSH/SFTP
Configuring vsftpd for Secure Connections
Setting up ProFTPd & TLS on Debian Etch
Filezilla - Free (GPL) FTP(S) & SFTP Client (Windows, Linux, OS X)

References

None

Severity	Name	Port	Category	Status
1	FTP Server Detection	21/tcp	FTP	Pass

Description

It is possible to obtain the banner of the remote FTP server by connecting to the remote port.

CVSS Score

0.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution

N/A

Details

The remote FTP banner is :

220-**********

220-Welcome to FTP

220-Please use your email address and password to login.

220-If you are registered for more than one site then your login name must be:
yourcompany.com/you@youremail.com.

220-**********

220-

220 FTP Server Ready

Links

None

References

None

Severity	Name	Port	Category	Status
1	TCP Timestamps	All	Other	Pass

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

CVSS Score

0.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution

n/a

Details

Synopsis :

The remote service implements TCP timestamps.

Description :

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See also :

http://www.ietf.org/rfc/rfc1323.txt

Solution :

n/a

Risk factor :

None

Links

www.ietf.org/rfc/rfc1323.txt

References

None

Severity	Name	Port	Category	Status
1	OS Identification	All	Other	Pass

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc...)
it is possible to guess the name of the remote operating system in use, and
sometimes its version

CVSS Score

0.0

CVSS Fingerprint

AV:N/AC:L/Au:N/C:N/I:N/A:N

Solution

By modifying the banners of the services running and blocking ICMP requests at the firewall, OS fingerprinting can be limited.

Details

Synopsis :

It is possible to guess the remote operating system

Description :

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc...)
it is possible to guess the name of the remote operating system in use, and
sometimes its version

Solution :

N/A

Risk factor :

None

Plugin output :

Remote operating system : Microsoft Windows Server 2008
Confidence Level : 75
Method : HTTP

Not all fingerprints could give a match - please email the following to os-signatures@ScanAlert.org :
HTTP:Server: Microsoft-IIS/7.0
SinFP:!:
P1:B11113:F0x12:W1608:O0:M0:
P2:B11113:F0x12:W4380:O0204ffff010303010101080affffffff4445414404020000:M1460:
P3:B00000:F0x00:W0:O0:M0
P4:3209_7_p=443R
SSLcert:!:i/CN:GlobalSign Domain Validation CAi/O:GlobalSign nv-
sas/CN:*.worldsecuresystems.coms/O:*.worldsecuresystems.com

The remote host is running Microsoft Windows Server 2008

Links

None

References

None

3.4.5 - Resolved: 202.176.14.137 / syd.worldsecuresystems.com (202.176.14.137)

None