Security Report - By Device

Larson Vitamins

11-JUL-2008 22:51

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.hackersafe.com.

Executive Summary

This report was generated by the SDP compliant scanning vendor McAfee, under certificate number 3709-01-01 in the framework of the PCI data security initiative and took into consideration security requirements as expressed in the MasterCard SDP Security Standard.

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.

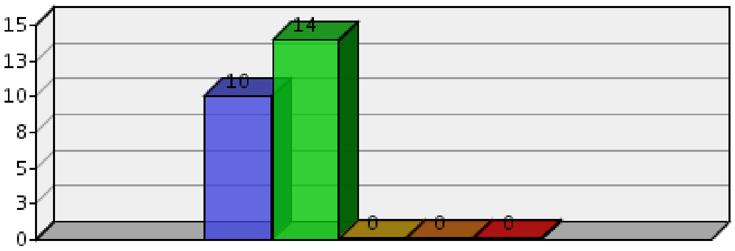
Report Overview

Customer Name	Larson Vitamins
Date Generated	11-JUL-2008 22:51
Report Type	Security - By Device
Devices	1
Device Groups	0
Vulnerabilities	12

Report Contents

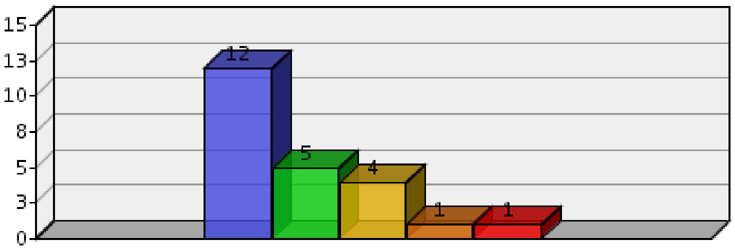
Vulnerabilities By Severity

		Severity
5	0	Urgent
4	0	Critical
3	0	High
2	14	Medium
1	10	Low



Vulnerabilities By Category (Top 5)

	Category
12	Web Application
5	General Remote Services
4	Web Server
1	Other
1	Backdoors / Trojans



Services Detected - All 1 Devices

Port	Protocol	Service	Devices
993	tcp	imaps	1
25	tcp	smtp	1
2096	tcp	Unknown	1
465	tcp	smtps	1
26	tcp	Unknown	1
2095	tcp	Unknown	1
2077	tcp	Unknown	1
2078	tcp	Unknown	1
110	tcp	pop-3	1
995	tcp	pop3s	1
22	tcp	ssh	1
2084	tcp	Unknown	1
143	tcp	imap2	1
2086	tcp	Unknown	1
2082	tcp	Unknown	1

2083	tcp	Unknown	1
1	tcp	tcpmux	1
80	tcp	http	1
2087	tcp	Unknown	1
443	tcp	https	1
21	tcp	ftp	1

All Vulnerabilities Found

	Name	Category	Devices
2	SSL Protocol Version 2 Detection	Web Application	1
2	Weak Supported Ssl Ciphers Suites	General Remote Services	1
2	Web Application Cross Site Scripting	Web Application	1
1	Potentially Sensitive Information Missing Secure Attribute in an Encrypted Session (SSL) Cookie	Web Application	1
1	Anonymous FTP Enabled	FTP	1
1	WebSite Directory Index	Web Server	1
1	SSH Protocol Versions Supported	Other	1
1	Missing Secure Attribute in an Encrypted Session (SSL) Cookie	Web Application	1
1	SMTP Server Detected on Non-standard Port	Backdoors / Trojans	1
1	Unencrypted Login Information Disclosure	Web Application	1
1	WebDAV Detection	Web Server	1
1	Apache UserDir Sensitive Information Disclosure	Web Server	1

Device Overview

Name	5 Urgent	4 Critical	3 High	2 Medium	1 Low	Open Ports
larsonvitamins.com	0	0	0	14	10	21

Overview - larsonvitamins.com

Last Audit Date	5 Urgent	4 Critical	3 High	2 Medium	1 Low	Total
11-JUL-2008 14:19	0	0	0	14	10	24

Open Ports - larsonvitamins.com

Port	Protocol	Service	Banner
1	tcp	tcpmux	null
21	tcp	ftp	ftp
22	tcp	ssh	null
25	tcp	smtp	smtp
26	tcp	Unknown	smtp
80	tcp	http	http
110	tcp	pop-3	pop3
143	tcp	imap2	imap
443	tcp	https	https
465	tcp	smtps	smtp
993	tcp	imaps	imap
995	tcp	pop3s	pop3
2077	tcp	Unknown	http
2078	tcp	Unknown	https
2082	tcp	Unknown	http
2083	tcp	Unknown	https
2084	tcp	Unknown	http
2086	tcp	Unknown	http
2087	tcp	Unknown	https
2095	tcp	Unknown	http
2096	tcp	Unknown	https

Vulnerabilities - larsonvitamins.com

2 SSL Protocol Version 2 Detection

Port	First Detected	Category
2096	11-APR-2008 08:17	Web Application
Protocol	**Fix Difficulty**	**Impact**
HTTPS	Medium	Information Disclosure

Description

The remote service appears to encrypt traffic using SSL protocol version 2.

Netscape Communications Corporation introduced SSL 2.0 with the launch of Netscape Navigator 1.0 in 1994 and it contains several well-known weaknesses. For example, SSLv2 doesn't provide any protection against man-in-the-middle attacks during the handshake, and uses the same cryptographic keys for message authentication and for encryption.

In Internet Explorer 7, the default HTTPS protocol settings are changed to disable the weaker SSLv2 protocol and to enable the stronger TLSv1 protocol. By default, IE7 users will only negotiate HTTPS connections using SSLv3 or TLSv1. Mozilla Firefox is expected to drop support for SSLv2 in its upcoming versions.

As almost all modern browsers support SSLv3, disabling support for the weaker SSL method should have minimal impact. The following browsers support SSLv3:

Internet Explorer 5.5 or higher (PC) Internet Explorer 5.0 or higher (Mac) Netscape 2.0 (Domestic) or higher (PC/Mac) Firefox 0.8 or higher (PC/Mac/Linux) Mozilla 1.7 or higher (PC/Mac/Linux) Camino 0.8 or higher (Mac) Safari 1.0 or higher (Mac) Opera 1.7 or higher (PC/Mac) Omniweb 3.0 or higher (Mac) Konqueror 2.0 or higher (Linux)

CVSS

5.0

Solution

Consult the application's documentation to disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead. Consult your documentation to identify how to reconfigure the affected application to avoid use of weak ciphers. Some knowledge base articles are listed below.

Apache Implementation:
In Apache, you need to modify the SSLCipherSuite directive in the httpd.conf or ssl.conf file. An example would be editing the following lines to something like:
SSLProtocol -ALL +SSLv3 +TLSv1
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:-LOW:-SSLv2:-EXP

More information can be read by clicking the Apache sslciphersuite directive information link below.

IIS Implementation:
Refer to the Microsoft KB Article on Disabling SSL 2.0, Article ID: 187498

Detail

None

Links

www.schneier.com/paper-ssl.html
Disable SSLv2 In IIS
Apache mod_ssl
IBM HTTP Server
SSL 2.0 IIS (Japanese)
IE Blog
Mozillazine

Related

None

2 SSL Protocol Version 2 Detection

Port	First Detected	Category
2087	11-APR-2008 08:17	Web Application
Protocol	**Fix Difficulty**	**Impact**
HTTPS	Medium	Information Disclosure

Description

The remote service appears to encrypt traffic using SSL protocol version 2.

Netscape Communications Corporation introduced SSL 2.0 with the launch of Netscape Navigator 1.0 in 1994 and it contains several well-known weaknesses. For example, SSLv2 doesn't provide any protection against man-in-the-middle attacks during the handshake, and uses the same cryptographic keys for message authentication and for encryption.

In Internet Explorer 7, the default HTTPS protocol settings are changed to disable the weaker SSLv2 protocol and to enable the stronger TLSv1 protocol. By default, IE7 users will only negotiate HTTPS connections using SSLv3 or TLSv1. Mozilla Firefox is expected to drop support for SSLv2 in its upcoming versions.

As almost all modern browsers support SSLv3, disabling support for the weaker SSL method should have minimal impact. The following browsers support SSLv3:

Internet Explorer 5.5 or higher (PC) Internet Explorer 5.0 or higher (Mac) Netscape 2.0 (Domestic) or higher (PC/Mac) Firefox 0.8 or higher (PC/Mac/Linux) Mozilla 1.7 or higher (PC/Mac/Linux) Camino 0.8 or higher (Mac) Safari 1.0 or higher (Mac) Opera 1.7 or higher (PC/Mac) Omniweb 3.0 or higher (Mac) Konqueror 2.0 or higher (Linux)

CVSS

5.0

Solution

Consult the application's documentation to disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead. Consult your documentation to identify how to reconfigure the affected application to avoid use of weak ciphers. Some knowledge base articles are listed below.

Apache Implementation:

In Apache, you need to modify the SSLCipherSuite directive in the httpd.conf or ssl.conf file. An example would be editing the following lines to something like:
SSLProtocol -ALL +SSLv3 +TLSv1
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:-LOW:-SSLv2:-EXP

More information can be read by clicking the Apache sslciphersuite directive information link below.

IIS Implementation:
Refer to the Microsoft KB Article on Disabling SSL 2.0, Article ID: 187498

Detail

None

Links

[www.schneier.com/paper-ssl.html]
[Disable SSLv2 In IIS]
[Apache mod_ssl]
[IBM HTTP Server]
[SSL 2.0 IIS (Japanese)]
[IE Blog]
[Mozillazine]

Related

None

2 SSL Protocol Version 2 Detection

Port	First Detected	Category
2083	11-APR-2008 08:17	Web Application
Protocol	**Fix Difficulty**	**Impact**
HTTPS	Medium	Information Disclosure

Description

The remote service appears to encrypt traffic using SSL protocol version 2.

Netscape Communications Corporation introduced SSL 2.0 with the launch of Netscape Navigator 1.0 in 1994 and it contains several well-known weaknesses. For example, SSLv2 doesn't provide any protection against man-in-the-middle attacks during the handshake, and uses the same cryptographic keys for message authentication and for encryption.

In Internet Explorer 7, the default HTTPS protocol settings are changed to disable the weaker SSLv2 protocol and to enable the stronger TLSv1 protocol. By default, IE7 users will only negotiate HTTPS connections using SSLv3 or TLSv1. Mozilla Firefox is expected to drop support for SSLv2 in its upcoming versions.

As almost all modern browsers support SSLv3, disabling support for the weaker SSL method should have minimal impact. The following browsers support SSLv3:

Internet Explorer 5.5 or higher (PC) Internet Explorer 5.0 or higher (Mac) Netscape 2.0 (Domestic) or higher (PC/Mac) Firefox 0.8 or higher (PC/Mac/Linux) Mozilla 1.7 or higher (PC/Mac/Linux) Camino 0.8 or higher (Mac) Safari 1.0 or higher (Mac) Opera 1.7 or higher (PC/Mac) Omniweb 3.0 or higher (Mac) Konqueror 2.0 or higher (Linux)

CVSS

5.0

Solution

Consult the application's documentation to disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead. Consult your documentation to identify how to reconfigure the affected application to avoid use of weak ciphers. Some knowledge base articles are listed below.

Apache Implementation:
In Apache, you need to modify the SSLCipherSuite directive in the httpd.conf or ssl.conf file. An example would be editing the following lines to something like:
SSLProtocol -ALL +SSLv3 +TLSv1
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:-LOW:-SSLv2:-EXP

More information can be read by clicking the Apache sslciphersuite directive information link below.

IIS Implementation:
Refer to the Microsoft KB Article on Disabling SSL 2.0, Article ID: 187498

Detail

None

Links

www.schneier.com/paper-ssl.html
Disable SSLv2 In IIS
Apache mod_ssl
IBM HTTP Server
SSL 2.0 IIS (Japanese)
IE Blog
Mozillazine

Related

None

2 SSL Protocol Version 2 Detection

Port	First Detected	Category
2078	11-APR-2008 08:17	Web Application
Protocol	**Fix Difficulty**	**Impact**
HTTPS	Medium	Information Disclosure

Description

The remote service appears to encrypt traffic using SSL protocol version 2.

Netscape Communications Corporation introduced SSL 2.0 with the launch of Netscape Navigator 1.0 in 1994 and it contains several well-known weaknesses. For example, SSLv2 doesn't provide any protection against man-in-the-middle attacks during the handshake, and uses the same cryptographic keys for message authentication and for encryption.

In Internet Explorer 7, the default HTTPS protocol settings are changed to disable the weaker SSLv2 protocol and to enable the stronger TLSv1 protocol. By default, IE7 users will only negotiate HTTPS connections using SSLv3 or TLSv1. Mozilla Firefox is expected to drop support for SSLv2 in its upcoming versions.

As almost all modern browsers support SSLv3, disabling support for the weaker SSL method should have minimal impact. The following browsers support SSLv3:

Internet Explorer 5.5 or higher (PC) Internet Explorer 5.0 or higher (Mac) Netscape 2.0 (Domestic) or higher (PC/Mac) Firefox 0.8 or higher (PC/Mac/Linux) Mozilla 1.7 or higher (PC/Mac/Linux) Camino 0.8 or higher (Mac) Safari 1.0 or higher (Mac) Opera 1.7 or higher (PC/Mac) Omniweb 3.0 or higher (Mac) Konqueror 2.0 or higher (Linux)

CVSS

5.0

Solution

Consult the application's documentation to disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead. Consult your documentation to identify how to reconfigure the affected application to avoid use of weak ciphers. Some knowledge base articles are listed below.

Apache Implementation:
In Apache, you need to modify the SSLCipherSuite directive in the httpd.conf or ssl.conf file. An example would be editing the following lines to something like:
SSLProtocol -ALL +SSLv3 +TLSv1
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:-LOW:-SSLv2:-EXP

More information can be read by clicking the Apache sslciphersuite directive information link below.

IIS Implementation:
Refer to the Microsoft KB Article on Disabling SSL 2.0, Article ID: 187498

Detail

None

Links

www.schneier.com/paper-ssl.html
Disable SSLv2 In IIS
Apache mod_ssl
IBM HTTP Server
SSL 2.0 IIS (Japanese)
IE Blog
Mozillazine

Related

None

2 SSL Protocol Version 2 Detection

Port	First Detected	Category
995	11-APR-2008 08:17	Web Application
Protocol	**Fix Difficulty**	**Impact**
HTTPS	Medium	Information Disclosure

Description

The remote service appears to encrypt traffic using SSL protocol version 2.

Netscape Communications Corporation introduced SSL 2.0 with the launch of Netscape Navigator 1.0 in 1994 and it contains several well-known weaknesses. For example, SSLv2 doesn't provide any protection against man-in-the-middle attacks during the handshake, and uses the same cryptographic keys for message authentication and for encryption.

In Internet Explorer 7, the default HTTPS protocol settings are changed to disable the weaker SSLv2 protocol and to enable the stronger TLSv1 protocol. By default, IE7 users will only negotiate HTTPS connections using SSLv3 or TLSv1. Mozilla Firefox is expected to drop support for SSLv2 in its upcoming versions.

As almost all modern browsers support SSLv3, disabling support for the weaker SSL method should have minimal impact. The following browsers support SSLv3:

Internet Explorer 5.5 or higher (PC) Internet Explorer 5.0 or higher (Mac) Netscape 2.0 (Domestic) or higher (PC/Mac) Firefox 0.8 or higher (PC/Mac/Linux) Mozilla 1.7 or higher (PC/Mac/Linux) Camino 0.8 or higher (Mac) Safari 1.0 or higher (Mac) Opera 1.7 or higher (PC/Mac) Omniweb 3.0 or higher (Mac) Konqueror 2.0 or higher (Linux)

CVSS

5.0

Solution

Consult the application's documentation to disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead. Consult your documentation to identify how to reconfigure the affected application to avoid use of weak ciphers. Some knowledge base articles are listed below.

Apache Implementation:
In Apache, you need to modify the SSLCipherSuite directive in the httpd.conf or ssl.conf file. An example would be editing the following lines to something like:
SSLProtocol -ALL +SSLv3 +TLSv1
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:-LOW:-SSLv2:-EXP

More information can be read by clicking the Apache sslciphersuite directive information link below.

IIS Implementation:
Refer to the Microsoft KB Article on Disabling SSL 2.0, Article ID: 187498

Detail

None

Links

www.schneier.com/paper-ssl.html
Disable SSLv2 In IIS
Apache mod_ssl
IBM HTTP Server
SSL 2.0 IIS (Japanese)
IE Blog
Mozillazine

Related

None

2 SSL Protocol Version 2 Detection

Port	First Detected	Category
993	11-APR-2008 08:17	Web Application
Protocol	**Fix Difficulty**	**Impact**
HTTPS	Medium	Information Disclosure

Description

The remote service appears to encrypt traffic using SSL protocol version 2.

Netscape Communications Corporation introduced SSL 2.0 with the launch of Netscape Navigator 1.0 in 1994 and it contains several well-known weaknesses. For example, SSLv2 doesn't provide any protection against man-in-the-middle attacks during the handshake, and uses the same cryptographic keys for message authentication and for encryption.

In Internet Explorer 7, the default HTTPS protocol settings are changed to disable the weaker SSLv2 protocol and to enable the stronger TLSv1 protocol. By default, IE7 users will only negotiate HTTPS connections using SSLv3 or TLSv1. Mozilla Firefox is expected to drop support for SSLv2 in its upcoming versions.

As almost all modern browsers support SSLv3, disabling support for the weaker SSL method should have minimal impact. The following browsers support SSLv3:

Internet Explorer 5.5 or higher (PC) Internet Explorer 5.0 or higher (Mac) Netscape 2.0 (Domestic) or higher (PC/Mac) Firefox 0.8 or higher (PC/Mac/Linux) Mozilla 1.7 or higher (PC/Mac/Linux) Camino 0.8 or higher (Mac) Safari 1.0 or higher (Mac) Opera 1.7 or higher (PC/Mac) Omniweb 3.0 or higher (Mac) Konqueror 2.0 or higher (Linux)

CVSS

5.0

Solution

Consult the application's documentation to disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead. Consult your documentation to identify how to reconfigure the affected application to avoid use of weak ciphers. Some knowledge base articles are listed below.

Apache Implementation:
In Apache, you need to modify the SSLCipherSuite directive in the httpd.conf or ssl.conf file. An example would be editing the following lines to something like:
SSLProtocol -ALL +SSLv3 +TLSv1
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:-LOW:-SSLv2:-EXP

More information can be read by clicking the Apache sslciphersuite directive information link below.

IIS Implementation:
Refer to the Microsoft KB Article on Disabling SSL 2.0, Article ID: 187498

Detail

None

Links

www.schneier.com/paper-ssl.html
Disable SSLv2 In IIS
Apache mod_ssl
IBM HTTP Server
SSL 2.0 IIS (Japanese)
IE Blog
Mozillazine

Related

None

2 SSL Protocol Version 2 Detection

Port	First Detected	Category
465	11-APR-2008 08:17	Web Application
Protocol	**Fix Difficulty**	**Impact**
HTTPS	Medium	Information Disclosure

Description

The remote service appears to encrypt traffic using SSL protocol version 2.

Netscape Communications Corporation introduced SSL 2.0 with the launch of Netscape Navigator 1.0 in 1994 and it contains several well-known weaknesses. For example, SSLv2 doesn't provide any protection against man-in-the-middle attacks during the handshake, and uses the same cryptographic keys for message authentication and for encryption.

In Internet Explorer 7, the default HTTPS protocol settings are changed to disable the weaker SSLv2 protocol and to enable the stronger TLSv1 protocol. By default, IE7 users will only negotiate HTTPS connections using SSLv3 or TLSv1. Mozilla Firefox is expected to drop support for SSLv2 in its upcoming versions.

As almost all modern browsers support SSLv3, disabling support for the weaker SSL method should have minimal impact. The following browsers support SSLv3:

Internet Explorer 5.5 or higher (PC) Internet Explorer 5.0 or higher (Mac) Netscape 2.0 (Domestic) or higher (PC/Mac) Firefox 0.8 or higher (PC/Mac/Linux) Mozilla 1.7 or higher (PC/Mac/Linux) Camino 0.8 or higher (Mac) Safari 1.0 or higher (Mac) Opera 1.7 or higher (PC/Mac) Omniweb 3.0 or higher (Mac) Konqueror 2.0 or higher (Linux)

CVSS

5.0

Solution

Consult the application's documentation to disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead. Consult your documentation to identify how to reconfigure the affected application to avoid use of weak ciphers. Some knowledge base articles are listed below.

Apache Implementation:
In Apache, you need to modify the SSLCipherSuite directive in the httpd.conf or ssl.conf file. An example would be editing the following lines to something like:
SSLProtocol -ALL +SSLv3 +TLSv1
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:-LOW:-SSLv2:-EXP

More information can be read by clicking the Apache sslciphersuite directive information link below.

IIS Implementation:
Refer to the Microsoft KB Article on Disabling SSL 2.0, Article ID: 187498

Detail

None

Links

www.schneier.com/paper-ssl.html
Disable SSLv2 In IIS
Apache mod_ssl
IBM HTTP Server
SSL 2.0 IIS (Japanese)
IE Blog
Mozillazine

Related

None

2 SSL Protocol Version 2 Detection

Port	First Detected	Category
443	11-APR-2008 08:17	Web Application
Protocol	**Fix Difficulty**	**Impact**
HTTPS	Medium	Information Disclosure

Description

The remote service appears to encrypt traffic using SSL protocol version 2.

Netscape Communications Corporation introduced SSL 2.0 with the launch of Netscape Navigator 1.0 in 1994 and it contains several well-known weaknesses. For example, SSLv2 doesn't provide any protection against man-in-the-middle attacks during the handshake, and uses the same cryptographic keys for message authentication and for encryption.

In Internet Explorer 7, the default HTTPS protocol settings are changed to disable the weaker SSLv2 protocol and to enable the stronger TLSv1 protocol. By default, IE7 users will only negotiate HTTPS connections using SSLv3 or TLSv1. Mozilla Firefox is expected to drop support for SSLv2 in its upcoming versions.

As almost all modern browsers support SSLv3, disabling support for the weaker SSL method should have minimal impact. The following browsers support SSLv3:

Internet Explorer 5.5 or higher (PC) Internet Explorer 5.0 or higher (Mac) Netscape 2.0 (Domestic) or higher (PC/Mac) Firefox 0.8 or higher (PC/Mac/Linux) Mozilla 1.7 or higher (PC/Mac/Linux) Camino 0.8 or higher (Mac) Safari 1.0 or higher (Mac) Opera 1.7 or higher (PC/Mac) Omniweb 3.0 or higher (Mac) Konqueror 2.0 or higher (Linux)

CVSS

5.0

Solution

Consult the application's documentation to disable SSL 2.0 and use SSL 3.0 or TLS 1.0 instead. Consult your documentation to identify how to reconfigure the affected application to avoid use of weak ciphers. Some knowledge base articles are listed below.

Apache Implementation:
In Apache, you need to modify the SSLCipherSuite directive in the httpd.conf or ssl.conf file. An example would be editing the following lines to something like:
SSLProtocol -ALL +SSLv3 +TLSv1

SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:-LOW:-SSLv2:-EXP

More information can be read by clicking the Apache sslciphersuite directive information link below.

IIS Implementation:
Refer to the Microsoft KB Article on Disabling SSL 2.0, Article ID: 187498

Detail

None

Links

www.schneier.com/paper-ssl.html
Disable SSLv2 In IIS
Apache mod_ssl
IBM HTTP Server
SSL 2.0 IIS (Japanese)
IE Blog
Mozillazine

Related

None

2 Weak Supported Ssl Ciphers Suites

Port	First Detected	Category
995	28-MAY-2008 20:39	General Remote Services
Protocol	**Fix Difficulty**	**Impact**
HTTP	Medium	Other

Description

The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.

CVSS

5.0

Solution

Consult your documentation to identify how to reconfigure the affected application to avoid use of weak ciphers. Some knowledge base articles are listed below.

IIS Implamentation:
In IIS you can require 128-bit encryption by checking the "Require 128-bit encryption" checkbox under the Directory Security tab. See IIS SSL Configuration link below. You could also disable specific ciphers by disabling their use in Windows. See the Restrict the Use of Certain Cryptographic Algorithms in Schannel.dll article.

Apache Implementation:
In Apache, you need to modify the SSLCipherSuite directive in the httpd.conf or ssl.conf file. An example would be editing it to something like, **"SSLCipherSuite ALL:-ADH:+HIGH:+MEDIUM:-LOW:-SSLv2:-EXP"**. More information can be read by clicking the Apache sslciphersuite directive information link below.

Detail

```
:

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

Low Strength Ciphers (< 56-bit key)
SSLv2
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
SSLv3
EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
TLSv1
EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export

The fields above are :

{OpenSSL ciphername}
```

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

Links

[Apache sslciphersuite directive information]()
[www.openssl.org]()
[Restrict the Use of Certain Cryptographic Algorithms in Schannel.dll]()
[IIS SSL Configuration]()

Related

None

2 Weak Supported Ssl Ciphers Suites

Port	First Detected	Category
993	28-MAY-2008 20:39	General Remote Services
Protocol	**Fix Difficulty**	**Impact**
HTTP	Medium	Other

Description

The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.

CVSS

5.0

Solution

Consult your documentation to identify how to reconfigure the affected application to avoid use of weak ciphers. Some knowledge base articles are listed below.

IIS Implementation:
In IIS you can require 128-bit encryption by checking the "Require 128-bit encryption" checkbox under the Directory Security tab. See IIS SSL Configuration link below. You could also disable specific ciphers by disabling their use in Windows. See the Restrict the Use of Certain Cryptographic Algorithms in Schannel.dll article.

Apache Implementation:
In Apache, you need to modify the SSLCipherSuite directive in the httpd.conf or ssl.conf file. An example would be editing it to something like, **"SSLCipherSuite ALL:-ADH:+HIGH:+MEDIUM:-LOW:-SSLv2:-EXP"**. More information can be read by clicking the Apache sslciphersuite directive information link below.

Detail

```
:

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

Low Strength Ciphers (< 56-bit key)
SSLv2
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
SSLv3
EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
TLSv1
EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export

The fields above are :

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

Links

Apache sslciphersuite directive information
www.openssl.org
Restrict the Use of Certain Cryptographic Algorithms in Schannel.dll
IIS SSL Configuration

Related

None

2 Weak Supported Ssl Ciphers Suites

Port	First Detected	Category
465	28-MAY-2008 20:39	General Remote Services
Protocol	**Fix Difficulty**	**Impact**
HTTP	Medium	Other

Description

The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.

CVSS

5.0

Solution

Consult your documentation to identify how to reconfigure the affected application to avoid use of weak ciphers. Some knowledge base articles are listed below.

IIS Implamentation:
In IIS you can require 128-bit encryption by checking the "Require 128-bit encryption" checkbox under the Directory Security tab. See IIS SSL Configuration link below. You could also disable specific ciphers by disabling their use in Windows. See the Restrict the Use of Certain Cryptographic Algorithms in Schannel.dll article.

Apache Implamentation:
In Apache, you need to modify the SSLCipherSuite directive in the httpd.conf or ssl.conf file. An example would be editing it to something like, **"SSLCipherSuite ALL:-ADH:+HIGH:+MEDIUM:-LOW:-SSLv2:-EXP"**. More information can be read by clicking the Apache sslciphersuite directive information link below.

Detail

```
:

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

Low Strength Ciphers (< 56-bit key)
SSLv2
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
SSLv3
EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
TLSv1
EXP-DES-CBC-SHA Kx=RSA(512) Au=RSA Enc=DES(40) Mac=SHA1 export
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export

The fields above are :

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

Links

Apache sslciphersuite directive information
www.openssl.org
Restrict the Use of Certain Cryptographic Algorithms in Schannel.dll
IIS SSL Configuration

Related

None

2 Weak Supported Ssl Ciphers Suites

Port	First Detected	Category
2078	28-JUN-2008 19:29	General Remote Services
Protocol	**Fix Difficulty**	**Impact**
HTTP	Medium	Other

Description

The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.

CVSS

5.0

Solution

Consult your documentation to identify how to reconfigure the affected application to avoid use of weak ciphers. Some knowledge base articles are listed below.

IIS Implamentation:
In IIS you can require 128-bit encryption by checking the "Require 128-bit encryption" checkbox under the Directory Security tab. See IIS SSL Configuration link below. You could also disable specific ciphers by disabling their use in Windows. See the Restrict the Use of Certain Cryptographic Algorithms in Schannel.dll article.

Apache Implamentation:
In Apache, you need to modify the SSLCipherSuite directive in the httpd.conf or ssl.conf file. An example would be editing it to something like, **"SSLCipherSuite ALL:-ADH:+HIGH:+MEDIUM:-LOW:-SSLv2:-EXP"**. More information can be read by clicking the Apache sslciphersuite directive information link below.

Detail

:

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

Low Strength Ciphers (< 56-bit key)
SSLv2
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export

The fields above are :

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

Links

[Apache sslciphersuite directive information]()
[www.openssl.org]()
[Restrict the Use of Certain Cryptographic Algorithms in Schannel.dll]()
[IIS SSL Configuration]()

Related

None

2 Weak Supported Ssl Ciphers Suites

Port	First Detected	Category
2087	06-JUL-2008 12:29	General Remote Services
Protocol	**Fix Difficulty**	**Impact**
HTTP	Medium	Other

Description

The remote host supports the use of SSL ciphers that offer either weak encryption or no encryption at all.

CVSS

5.0

Solution

Consult your documentation to identify how to reconfigure the affected application to avoid use of weak ciphers. Some knowledge base articles are listed below.

IIS Implamentation:
In IIS you can require 128-bit encryption by checking the "Require 128-bit encryption" checkbox under the Directory Security tab. See IIS SSL Configuration link below. You could also disable specific ciphers by disabling their use in Windows. See the Restrict the Use of Certain Cryptographic Algorithms in Schannel.dll article.

Apache Implamentation:
In Apache, you need to modify the SSLCipherSuite directive in the httpd.conf or ssl.conf file. An example would be editing it to something like, **"SSLCipherSuite ALL:-ADH:+HIGH:+MEDIUM:-LOW:-SSLv2:-EXP"**. More information can be read by clicking the Apache sslciphersuite directive information link below.

Detail

```
:

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

Low Strength Ciphers (< 56-bit key)
SSLv2
EXP-RC2-CBC-MD5 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
EXP-RC4-MD5 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export

The fields above are :

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

Links

[Apache sslciphersuite directive information]
[www.openssl.org]
[Restrict the Use of Certain Cryptographic Algorithms in Schannel.dll]
[IIS SSL Configuration]

Related

None

2 Web Application Cross Site Scripting

Port	First Detected	Category
80	11-JUL-2008 14:19	Web Application
Protocol	**Fix Difficulty**	**Impact**
HTTP	Medium	Cross Site Scripting (XSS)

Description

The remote web application appears to be vulnerable to cross-site scripting (XSS).

The cross-site scripting attack is one of the most common, yet overlooked, security problems facing web developers today. A web site is vulnerable if it displays user-submitted content without sanitizing user input.

The target of cross-site scripting attacks is not the server itself, but the users of the server. By finding a page that does not properly sanitize user input the attacker submits client-side code to the server that will then be rendered by the client. It is important to note that websites that use SSL are just as vulnerable as websites that do not encrypt browser sessions.

The damage caused by such an attack can range from stealing session and cookie data from your customers to loading a virus payload onto their computer via browser.

The pages listed in the vulnerability output will display embedded javascript with no filtering back to the user.

CVSS

5.8

Solution

When accepting user input ensure that you are HTML encoding potentially malicious characters if you ever display the data back to the client.

Ensure that parameters and user input are sanitized by doing the following:
Remove < input and replace with &lt;
Remove > input and replace with &gt;
Remove ' input and replace with &apos;
Remove " input and replace with &#x22;
Remove) input and replace with &#x29;
Remove (input and replace with &#x28;

Detail

Protocol	http	Port	80	Read Timeout	10000	Method	POST
Path	/customer.php						
Query	%22Xx%3CXaXaXXaXaX%3ExX=custregister update=false						
Headers	Referer= Content-Type=application%2Fx-www-form-urlencoded						
Body	posted=>"></title></iframe></script></form></td></tr><br><iFraMe src=http://www.HackerSafe.com width=900 height=1100></IfRamE> fl=0 email=0 password=0 remember=1 imgsubmit=0						

Protocol	http	Port	80	Read Timeout	10000	Method	POST
Path	/customer.php						
Query	%22Xx%3CXaXaXXaXaX%3ExX=custregister update=false						
Headers	Referer= Content-Type=application%2Fx-www-form-urlencoded						
Body	posted=1 fl=>"></title></iframe></script></form></td></tr><br><iFraMe src=http://www.HackerSafe.com width=900 height=1100></IfRamE> email=0 password=0 remember=1 imgsubmit=0						

Protocol	http	Port	80	Read Timeout	10000	Method	POST
Path	/customer.php						
Query	%22Xx%3CXaXaXXaXaX%3ExX=custregister update=false						
Headers	Referer= Content-Type=application%2Fx-www-form-urlencoded						
Body	posted=1 fl=0 email=>"></title></iframe></script></form></td></tr><br><iFraMe src=http://www.HackerSafe.com width=900 height=1100></IfRamE> password=0 remember=1 imgsubmit=0						

Protocol	http	Port	80	Read Timeout	10000	Method	POST
Path	/customer.php						
Query	%22Xx%3CXaXaXXaXaX%3ExX=custregister update=false						
Headers	Referer= Content-Type=application%2Fx-www-form-urlencoded						
Body	posted=1 fl=0 email=0 password=>"></title></iframe></script></form></td></tr><br><iFraMe src=http://www.HackerSafe.com width=900 height=1100></IfRamE> remember=1 imgsubmit=0						

Protocol	http	Port	80	Read Timeout	10000	Method	POST
Path	/customer.php						
Query	%22Xx%3CXaXaXXaXaX%3ExX=custregister update=false						
Headers	Referer= Content-Type=application%2Fx-www-form-urlencoded						
Body	posted=1 fl=0 email=0 password=0 remember=>"></title></iframe></script></form></td></tr> <iFraMe src=http://www.HackerSafe.com width=900 height=1100></IfRamE> imgsubmit=0						

Protocol	http	Port	80	Read Timeout	10000	Method	POST
Path	/customer.php						
Query	%22Xx%3CXaXaXXaXaX%3ExX=custregister update=false						
Headers	Referer= Content-Type=application%2Fx-www-form-urlencoded						
Body	posted=1 fl=0 email=0 password=0 remember=1 imgsubmit=>"></title></iframe></script></form></td></tr> <iFraMe src=http://www.HackerSafe.com width=900 height=1100></IfRamE>						

Protocol	http	Port	80	Read Timeout	10000	Method	POST
Path	/customer.php						
Query	%22Xx%3CXaXaXXaXaX%3ExX=custregister update=false						
Headers	Referer= Content-Type=application%2Fx-www-form-urlencoded						
Body	>"><script>alert(123)</script><"=1 fl=0 email=0 password=0 remember=1 imgsubmit=0						

Protocol	http	Port	80	Read Timeout	10000	Method	POST
Path	/customer.php						
Query	%22Xx%3CXaXaXXaXaX%3ExX=custregister update=false						
Headers	Referer= Content-Type=application%2Fx-www-form-urlencoded						
Body	posted=1 >"><script>alert(123)</script><"=0 email=0 password=0 remember=1 imgsubmit=0						

Protocol	http	Port	80	Read Timeout	10000	Method	POST
Path	/customer.php						
Query	%22Xx%3CXaXaXXaXaX%3ExX=custregister update=false						
Headers	Referer= Content-Type=application%2Fx-www-form-urlencoded						
Body	posted=1 fl=0 >"><script>alert(123)</script><"=0 password=0 remember=1						

	imgsubmit=0

Protocol	http **Port** 80 **Read Timeout** 10000 **Method** POST
Path	/customer.php
Query	%22Xx%3CXaXaXXaXaX%3ExX=custregister update=false
Headers	Referer= Content-Type=application%2Fx-www-form-urlencoded

Body	posted=1
	fl=0
	email=0
	>"><script>alert(123)</script><"=0
	remember=1
	imgsubmit=0

Links

OWASP XSS Description and Solution
www.owasp.org/documentation/guide
www.vnunet.com/vnunet/news/2116667/top-sites-vulnerable-hackers
www.cgisecurity.com/articles/xss-faq.shtml
www.technicalinfo.net/papers/CSS.html
Top sites vulnerable to hackers
An Oldie but Goodie: The Cross-Site Scripting Vulnerability
Apache: ???
Apache: Cross Site Scripting Info
www.developer.com/lang/article.php/947041
The Cross Site Scripting FAQ
sandsprite.com/Sleuth/papers/RealWorld_XSS_1.html
www.cert.org/tech_tips/malicious_code_FAQ.html
OWASP XSS
The Cross-Site Scripting Vulnerability
Top sites vulnerable to hackers

Related

CERT	CA-2000-02

Information Disclosures - larsonvitamins.com

1 SMTP Server Detected on Non-standard Port

Port	First Detected	Category
26	11-APR-2008 08:17	Backdoors / Trojans
Protocol	**Fix Difficulty**	**Impact**
SMTP	Medium	Other

Description

This SMTP server appears to be running on a non-standard port.

Alternate SMTP ports are common due to the fact that an increasing number of ISP's and firewall configurations block outgoing mail / SMTP connections on port 25 (the standard SMTP port), enroute to their web/email providers. These non-standard ports are open on many web servers in order for legitimate senders to have the ability to relay through a mail server other than the one run by their ISP.

However, this can cause problems when you need use an SMTP other than the provider's (their servers may be unreliable or overly restrictive), or if they block port 25 but do not provide SMTP service themselves.

CVSS

0.0

Solution

Verify whether the alternate SMTP port is part of your normal configuration. If this is the case, you will need to manually resolve this item. If not, you will need to track down the process that's using this port and disable it. One way to identify processes and their corresponding ports in Linux is to issue the 'netstat' command. For RedHat, Centos, and Fedora, the commandline would be 'netstat -tulp'. The output would look similar to the following:

```
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
```

```
tcp 0 0 *:smtp *:* LISTEN 17648/tcpserver
tcp 0 0 *:26 *:* LISTEN 17713/tcpserver
```

Notice tcpserver(qmail) is using both port 25 and 26 in this example. The number next to 'tcpserver' is the process ID. If you see an smtp process that is not supposed to be running, you can kill it by typing: 'kill PID'. Using the example above, you would type 'kill 17713'. After that, you can run netstat once more to check for the presence of that process. If the kill command does not remove the process, run this command: 'kill -9 PID'. This is the force command for 'kill'.

If the rogue process persists, seek the help of a qualified administrator. At this point, you should assume that the server may have been compromised. A full security sweep is strongly recommended.

If there is proof of a compromise, contact ScanAlert immediately. We will assist you in the remediation process.

Detail

None

Links

None

Related

None

1 SSH Protocol Versions Supported

Port	First Detected	Category
22	11-APR-2008 08:17	Other
Protocol	**Fix Difficulty**	**Impact**
SSH	Medium	Information Disclosure

Description

We were able to determine which versions of the SSH protocol the remote SSH daemon supports.

This gives potential attackers additional information about the system they are attacking.

CVSS

0.0

Solution

No solution is required.

Detail

The remote SSH daemon supports the following versions of the
SSH protocol :

. 1.99
. 2.0

SSHv2 host key fingerprint : 8b:7e:7e:df:b3:62:6a:7d:c2:c5:52:2f:a5:9b:05:e0

Links

www.openssh.org

Related

None

1 Anonymous FTP Enabled

Port	First Detected	Category
21	11-APR-2008 08:17	FTP
Protocol	**Fix Difficulty**	**Impact**
FTP	Medium	Remote File Access

Description

The FTP service appears to allow anonymous logins.

ScanAlert normally recommends disabling anonymous access to your FTP server, since many ftp applications do not provide proper safeguards. However, anonymous FTP can be a valuable service if correctly configured and administered.

Some anonymous FTP sites are used to transfer copyrighted material, as well as deliberately transferring excess amounts of files to cause a denial of service. In some cases, anonymous FTP users can compromise the system if improperly configured.

CVSS

5.0

Solution

If you need anonymous logins, ensure that the anonymous user has minimal filesystem permissions. Under most Unix systems, to fix this execute:

echo ftp >> /etc/ftpusers

Another useful practice is limiting the amount of data transferred in one session. Also control the overall amount of data transferred based on available disk space. If possible, dedicate a disk drive to this task. If the dedicated disk becomes full, it will not cause a denial of service problem.

Two secure FTP applications available for Unix-like systems are pure-ftpd and vsftpd:
http://www.pureftpd.org/project/pure-ftpd
http://vsftpd.beasts.org/

See Links section for detailed anonymous ftp guidelines.

Detail

None

Links

Anonymous FTP Abuses
Anonymous FTP Configuration Guidelines
xforce.iss.net/static/543.php
xforce.iss.net/static/52.php

Related

CVE CVE-1999-0497

1 WebSite Directory Index

Port	First Detected	Category
443	11-JUL-2008 14:19	Web Server
Protocol	**Fix Difficulty**	**Impact**
HTTP	Medium	Remote File Access

Description

This script attempts to retrieve a directory listing of common directories.

CVSS

5.0

Solution

If you do not want the public to access your directories, place a blank index page in each directory in question. Another alternative, would be to password protect the directory.

Detail

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

/Scripts

Links

OWASP

Related

Other OWASP-CM-004

1 Apache UserDir Sensitive Information Disclosure

Port	First Detected	Category
443	11-JUL-2008 14:19	Web Server
Protocol	**Fix Difficulty**	**Impact**
HTTP	Medium	Information Disclosure

Description

The remote Apache server can be used to guess the presence of a given user name on the remote host.

An information leak occurs, due to a configuration error, on Apache based web servers whenever the UserDir module is enabled. Requests to URLs containing a tilde followed by a username will redirect the user to a given subdirectory in the user home. Installations with this default misconfiguration allow remote users to determine whether a give username exists on the remote system.

The following example is proof of concept:

http://www.example.com/~foo
1. If user 'foo' exists, the HTTP result code will be 200, and foo's homepage will load in the browser.
2. If user 'foo' exists, but access is restricted, the HTTP result code will be 403, with the following message from Apache: "You don't have permission to access /~foo on this server."
3. If 'foo' does not exist, the HTTP result code will be 404, with the following message from Apache: "The requested URL /~foo was not found on this server".

Properly exploited, this information could be used to initiate specific attacks against a given system.

CVSS

5.0

Solution

1) Disable this feature by changing 'UserDir public_html' to 'UserDir disabled'.

Or

2) Use a RedirectMatch rewrite rule under Apache -- this works even if there is no such entry in the password file, e.g.:
RedirectMatch ^/~(.*)$ http://my-target-webserver.somewhere.org/$1

Or

3) Add into httpd.conf:
ErrorDocument 404 http://servername.com/sample.html
ErrorDocument 403 http://servername.com/sample.html
NOTE: **You need to use a FQDN inside the URL for it to work properly.**

Detail

Request:StatusCode ---> /~root : 403 ; /~admin : 404 ; /~ScanAlert1234567890 : 404

Links

www.securiteam.com/unixfocus/5WP0C1F5FI.html
Apache?????
www.securiteam.com/unixfocus/5WP0C1F5FI.html

Related

CVE	CVE-2001-1013
BugTraq	3335
Open Source Vulnerability Database	637

1 Missing Secure Attribute in an Encrypted Session (SSL) Cookie

Port	First Detected	Category
443	11-JUL-2008 14:19	Web Application
Protocol	**Fix Difficulty**	**Impact**
HTTPS	Medium	Information Disclosure

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

0.0

Solution

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

Detail

Path: / --> No "Secure" Attribute on Secure Channel (https) :
PHPSESSID=c9df2ab244b0bb11698dca174439f489; path=/

Links

Persistent Client State HTTP Cookies
RFC 2109 - HTTP State Management Mechanism
IPA ??????????
Microsoft

Related

None

1 Potentially Sensitive Information Missing Secure Attribute in an Encrypted Session (SSL) Cookie

Port	First Detected	Category
443	11-JUL-2008 14:19	Web Application
Protocol	**Fix Difficulty**	**Impact**
HTTP	Medium	Information Disclosure

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

2.1

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.

Detail

Path: / --> Sensitive Info on secure Channel (https) without "Secure" Attribute :
PHPSESSID=c9df2ab244b0bb11698dca174439f489; path=/

Links

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

Related

CVE CVE-2004-0462

1 WebDAV Detection

Port	First Detected	Category
443	11-JUL-2008 14:19	Web Server
Protocol	**Fix Difficulty**	**Impact**
HTTP	Medium	Information Disclosure

Description

The remote server appears to be running with WebDAV enabled. This is a very dangerous service to have publicly available as it has many security flaws and is often target by hackers.

WebDAV is an industry standard extension to the HTTP specification. It adds a capability for authorized users to remotely add and manage the content of a web server.

This extention should be disabled.

CVSS

0.0

Solution

Disable WebDAV if its not absolutely needed.

To disable in IIS 5, install and configure Microsoft's IISLockdown.

Windows 2003/IIS 6:
WebDAV is disabled by default.

To disable in Apache do the following:
In the httpd.conf, comment out the entry for 'mod_dav.c' and the corresponding 'LoadModule' directive. Restart httpd

Detail

WebDAV enabled

Links

IIS Lockdown
WebDAV????????
Securing WebDAV in IIS 6
Enabling or Disabling WebDAV Per Web Site
IIS Lockdown

Related

None

1 WebSite Directory Index

Port	First Detected	Category
80	11-JUL-2008 14:19	Web Server
Protocol	**Fix Difficulty**	**Impact**
HTTP	Medium	Remote File Access

Description

This script attempts to retrieve a directory listing of common directories.

CVSS

5.0

Solution

If you do not want the public to access your directories, place a blank index page in each directory in question. Another alternative, would be to password protect the directory.

Detail

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

/Scripts

Links

OWASP

Related

Other OWASP-CM-004

1 Unencrypted Login Information Disclosure

Port	First Detected	Category
80	11-JUL-2008 14:19	Web Application
Protocol	**Fix Difficulty**	**Impact**
HTTP	Medium	Information Disclosure

Description

The remote host appears to allow logins over unencrypted (HTTP) connections. This means that a user's login information is sent over the internet in clear text. An attacker may be able to uncover login names and passwords by sniffing network traffic.

Solution

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

Detail

Protocol	http	Port	80	Read Timeout	10000	Method	POST

Path	/customer.php
Query	%22Xx%3CXaXaXXaXaX%3ExX=custregister update=false

Headers	Referer=http%3A%2F%2Flarsonvitamins.com%3A80%2Fcustomer.php%3F%2522Xx%253CXaXaXXaXaX%253ExX%3Dcustregister%26update%3Dfalse
	Content-Type=application%2Fx-www-form-urlencoded

Body	posted=1
	fl=
	email=ScanAlertUserName
	password=ScanAlertPassword
	remember=1
	imgsubmit=

Form name: None

Links

None

Related

None

None

Resolved Items - larsonvitamins.com

None

Vulnerability Levels

Severity	Level	Description
5	Urgent	Intruders can easily gain control of the device being tested, which can lead to the compromise of your entire network security. Or hackers can use this device to access sensitive information from other devices in your network. Hackers are often actively scanning for this type of vulnerability. For example, vulnerabilities at this level may include full read and write access to files or databases, remote execution of commands, gaining Administrator or Root level access, and the presence of Trojans or backdoors.
4	Critical	Intruders can possibly gain direct control of the device being tested, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users hosted on the device.
3	High	Intruders may be able to gain access to specific information stored on the device being tested, including security settings. This could result in potential misuse of, or unauthorized access to the device or information stored on it. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services such as mail-relaying.
2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of OS or software installed or directory structure. While this level of vulnerability is not directly exploitable itself, with this information intruders can more easily exploit possible vulnerabilities specific to software versions in use.
1	Low	Intruders can collect general information about the device being tested (open ports, OS or software type, etc.). Hackers may be able to use this information to find exploitable vulnerabilities.