List of hosts

192.168.1.10	Medium Severity problem(s) found

[^] Back

192.168.1.10

Scan Time

Start time :	Fri May 14 19:16:46 2010
End time :	Fri May 14 19:18:24 2010

Number of vulnerabilities

Open ports :	11
High :	0
Medium :	8
Low :	36

Remote host information

Operating System :	Linux Kernel 2.6 on CentOS 4
NetBIOS name :	
DNS name :	

[^] Back to 192.168.1.10

Port general (0/icmp) [-/+]

Traceroute Information

Synopsis:
It was possible to obtain
traceroute information.

Description:
Makes a traceroute
to the remote host.

Risk factor:
None

Solution:
n/a

Plugin output:
For your information, here is the traceroute from
192.168.1.2 to 192.168.1.10 :
192.168.1.2
192.168.1.10

Plugin ID:
10287

Nessus Scan Information

Information about this scan :

Nessus version : 4.2.2
Plugin feed version : 201005140034
Type of plugin feed : ProfessionalFeed (Direct)
Scanner IP : 192.168.1.2
Port scanner(s) : nessus_tcp_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : Detected
Scan Start Date : 2010/5/14 19:16
Scan duration : 98 sec

Plugin ID:
19506

Web Application Tests Disabled

Synopsis:
Web application tests were
not enabled during the scan.

Description:
One or
several web servers were detected by Nessus, but neither the
CGI tests nor the Web Application Tests were enabled.

If you want to get a more complete report, you should enable one of
these features, or both.

Please note that the scan might take significantly longer with these
tests, which is why they are disabled by default.

Risk factor:
None

**See
also:**
http://blog.tenablesecurity.com/web-app-auditing/

Solution:
To
enable specific CGI tests, go to the 'Advanced' tab, select
'Global variable settings' and set 'Enable CGI scanning'.

To generic enable web application tests, go to the 'Advanced' tab,
select 'Web Application Tests Settings' and set 'Enable web
applications tests'.

You may configure other options, for example HTTP credentials in
'Login configurations', or form-based authentication in 'HTTP login
page'.

Plugin ID:
43067

Common Platform Enumeration (CPE)

Synopsis:
It is possible to
enumerate CPE names that matched on the remote
system.

Description:
By using information obtained from
a Nessus scan, this plugin reports
CPE (Common Platform Enumeration) matches for various hardware and
software products found on a host.

Note that if an official CPE is not available for the product, this
plugin computes the best possible CPE based on the information
available from the scan.

Risk factor:
None

**See
also:**
http://cpe.mitre.org/

Solution:
n/a

**Plugin
output:**

The remote operating system matched the following CPE :

cpe:/o:centos:centos:4 -> CentOS-4

Here is the list of application CPE IDs that matched on the remote
system :

cpe:/a:apache:http_server:2.0.52 -> Apache Software Foundation
Apache HTTP Server 2.0.52
cpe:/a:apache:http_server:2.0.52 -> Apache Software Foundation
Apache HTTP Server 2.0.52

Plugin ID:
45590

OS Identification

Remote operating system : Linux Kernel 2.6 on CentOS 4
Confidence Level : 95
Method : HTTP

The remote host is running Linux Kernel 2.6 on CentOS 4

**Plugin
ID:**
11936

Apache Banner Linux Distribution Disclosure

Synopsis:
The name of the Linux
distribution running on the remote host was
found in the banner of the web server.

Description:
This
script extracts the banner of the Apache web server and attempts
to determine which Linux distribution the remote host is running.

**Risk
factor:**
None

Solution:
If you do not wish to
display this information, edit httpd.conf and
set the directive 'ServerTokens Prod' and restart Apache.

**Plugin
output:**

The linux distribution detected was :
- CentOS 4

Plugin ID:
18261

Ethernet card brand

Synopsis:
The manufacturer can be
deduced from the Ethernet OUI.

Description:
Each
ethernet MAC address starts with a 24-bit 'Organizationally
Unique Identifier'.
These OUI are registered by IEEE.

Risk factor:
None

**See
also:**
http://standards.ieee.org/faqs/OUI.html

**See
also:**
http://standards.ieee.org/regauth/oui/index.shtml

Solution:
n/a

**Plugin
output:**

The following card manufacturers were identified :

00:13:72:xx:xx:xx : Dell Inc.

Plugin ID:
35716

TCP/IP Timestamps Supported

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.

Risk factor:
None

**See
also:**
http://www.ietf.org/rfc/rfc1323.txt

Solution:
n/a

**Plugin
ID:**
25220

ICMP Timestamp Request Remote Date Disclosure

Synopsis:
It is possible to
determine the exact time set on the remote host.

Description:
The
remote host answers to an ICMP timestamp request. This allows an
attacker to know the date which is set on your machine.

This may help him to defeat all your time based authentication
protocols.

Risk factor:
None

Solution:
Filter
out the ICMP timestamp requests (13), and the outgoing ICMP
timestamp replies (14).

Plugin output:
The difference
between the local and remote clocks is -622 seconds.

Plugin ID:
10114

CVE:

CVE-1999-0524

Other references:
OSVDB:94

Port rpc-portmapper (111/tcp) [-/+]

RPC Services Enumeration

Synopsis:
An ONC RPC service is
running on the remote host.

Description:
By sending a
DUMP request to the portmapper, it was possible to
enumerate the ONC RPC services running on the remote port. Using this
information, it is possible to connect and bind to each service by
sending an RPC request to the remote port.

Risk factor:
None

Solution:
n/a

**Plugin
output:**

The following RPC services are available on UDP port 111 :

- program: 100000 (portmapper), version: 2

Plugin ID:
11111

RPC portmapper Service Detection

Synopsis:
An ONC RPC portmapper is
running on the remote host.

Description:
The RPC
portmapper is running on this port.

The portmapper allows someone to get the port number of each RPC
service running on the remote host by sending either multiple lookup
requests or a DUMP request.

Risk factor:
None

Solution:
n/a

**Plugin
ID:**
10223

RPC Services Enumeration

Synopsis:
An ONC RPC service is
running on the remote host.

Description:
By sending a
DUMP request to the portmapper, it was possible to
enumerate the ONC RPC services running on the remote port. Using this
information, it is possible to connect and bind to each service by
sending an RPC request to the remote port.

Risk factor:
None

Solution:
n/a

**Plugin
output:**

The following RPC services are available on TCP port 111 :

- program: 100000 (portmapper), version: 2

Plugin ID:
11111

Port ssh (22/tcp) [-/+]

SSH Protocol Version 1 Session Key Retrieval

Synopsis:
The remote service offers
an insecure cryptographic protocol.

Description:
The
remote SSH daemon supports connections made using the version 1.33
and/or 1.5 of the SSH protocol.

These protocols are not completely cryptographically safe so they
should not be used.

Risk factor:
Medium

CVSS
Base Score:4.0
CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:N

Solution:
Disable
compatibility with version 1 of the protocol.

Plugin ID:
10882

CVE:

CVE-2001-0361

BID:
2344

**Other
references:**
OSVDB:2116

Backported Security Patch Detection (SSH)

Synopsis:
Security patches are
backported.

Description:
Security patches may have been
'back ported' to the remote SSH server
without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any
security problem.

Risk factor:
None

See also:
http://www.nessus.org/u?d636c8c7

Solution:
N/A

**Plugin
output:**
Give Nessus credentials to perform local checks.

**Plugin
ID:**
39520

SSH Protocol Versions Supported

Synopsis:
A SSH server is running on
the remote host.

Description:
This plugin determines
the versions of the SSH protocol supported by
the remote SSH daemon.

Risk factor:
None

Solution:
n/a

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

- 1.33
- 1.5
- 1.99
- 2.0

SSHv1 host key fingerprint :
6e:b8:db:35:4d:c9:57:1f:83:57:ee:52:c5:a2:7e:b9
SSHv2 host key fingerprint :
ec:cd:97:9f:94:96:af:df:eb:b4:3a:da:2f:ed:f8:75

Plugin ID:
10881

SSH Server Type and Version Information

Synopsis:
An SSH server is listening
on this port.

Description:
It is possible to obtain
information about the remote SSH
server by sending an empty authentication request.

Risk factor:
None

Solution:
n/a

Plugin output:

SSH version : SSH-1.99-OpenSSH_3.9p1
SSH supported authentication : publickey,gssapi-with-mic,password

Plugin ID:
10267

Service Detection

An SSH server is running on this port.

Plugin ID:
22964

Port www (443/tcp) [-/+]

Web Server Expect Header XSS

Synopsis:
The remote web server is
vulnerable to a cross-site scripting attack.

Description:
The
remote web server fails to sanitize the contents of an 'Expect'
request header before using it to generate dynamic web content. An
unauthenticated remote attacker may be able to leverage this issue to
launch cross-site scripting attacks against the affected service,
perhaps through specially-crafted ShockWave (SWF) files.

**Risk
factor:**
Medium

CVSS Base Score:4.3
CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

**See
also:**
http://archives.neohapsis.com/archives/bugtraq/2006-05/0151.html

**See
also:**
http://archives.neohapsis.com/archives/bugtraq/2006-05/0441.html

**See
also:**
http://archives.neohapsis.com/archives/bugtraq/2006-07/0425.html

**See
also:**
http://www.apache.org/dist/httpd/CHANGES_2.2

**See
also:**
http://www.apache.org/dist/httpd/CHANGES_2.0

**See
also:**
http://www.apache.org/dist/httpd/CHANGES_1.3

**See
also:**
http://www-1.ibm.com/support/docview.wss?uid=swg1PK24631

**See
also:**
http://www-1.ibm.com/support/docview.wss?uid=swg24017314

Solution:
Check
with the vendor for an update to the web server. For Apache,
the issue is reportedly fixed by versions 1.3.35 / 2.0.57 / 2.2.2; for
IBM HTTP Server, upgrade to 6.0.2.13 / 6.1.0.1; for IBM WebSphere
Application Server, upgrade to 5.1.1.17.

Plugin output:

Nessus was able to exploit the issue using the following request :

---------- snip ----------
GET / HTTP/1.1

HTTP TRACE / TRACK Methods Allowed

Synopsis:
Debugging functions are
enabled on the remote web server.

Description:
The
remote webserver supports the TRACE and/or TRACK methods. TRACE
and TRACK are HTTP methods that are used to debug web server
connections.

Risk factor:
Medium

CVSS Base
Score:4.3
CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N

See also:
http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

See
also:
http://www.apacheweek.com/issues/03-01-24

See
also:
http://www.kb.cert.org/vuls/id/288308

See also:
http://www.kb.cert.org/vuls/id/867593

See
also:
http://sunsolve.sun.com/search/document.do?assetkey=1-66-200942-1

Solution:
Disable
these methods. Refer to the plugin output for more information.

Plugin
output:

To disable these methods, add the following lines for each virtual
host in your configuration file :

RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request :

---------- snip ----------
TRACE /Nessus335020682.html HTTP/1.1
Connection: Close
Host: 192.168.1.10
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1;
Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png,

SSL Version 2 (v2) Protocol Detection

Synopsis:
The remote service
encrypts traffic using a protocol with known
weaknesses.

Description:
The remote service accepts
connections encrypted using SSL 2.0, which
reportedly suffers from several cryptographic flaws and has been
deprecated for several years. An attacker may be able to exploit
these issues to conduct man-in-the-middle attacks or decrypt
communications between the affected service and clients.

**Risk
factor:**
Medium

CVSS Base Score:5.0
CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

**See
also:**
http://www.schneier.com/paper-ssl.pdf

See also:
http://support.microsoft.com/kb/187498

**See
also:**
http://www.linux4beginners.info/node/disable-sslv2

Solution:
Consult
the application's documentation to disable SSL 2.0 and use SSL
3.0 or TLS 1.0 instead.

Plugin ID:
20007

SSL Weak Cipher Suites Supported

Synopsis:
The remote service
supports the use of weak SSL ciphers.

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

Risk factor:
Medium

CVSS
Base Score:5.0
CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

See
also:
http://www.openssl.org/docs/apps/ciphers.html

Solution:
Reconfigure
the affected application if possible to avoid use of weak
ciphers.

Plugin output:
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-EDH-RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES(40)
Mac=SHA1 export
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-EDH-RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES(40)
Mac=SHA1 export
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}

SSL Medium Strength Cipher Suites Supported

Synopsis:
The remote service
supports the use of medium strength SSL ciphers.

Description:
The
remote host supports the use of SSL ciphers that offer medium
strength encryption, which we currently regard as those with key
lengths at least 56 bits and less than 112 bits.

Risk factor:
Medium

CVSS
Base Score:5.0
CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Solution:
Reconfigure
the affected application if possible to avoid use of
medium strength ciphers.

Plugin output:

Here are the medium strength SSL ciphers supported by the remote server :

Medium Strength Ciphers (>= 56-bit and < 112-bit key)
SSLv2
DES-CBC-MD5 Kx=RSA Au=RSA Enc=DES(56)
Mac=MD5
RC4-64-MD5 Kx=RSA Au=RSA Enc=RC4(64)
Mac=MD5
SSLv3
EDH-RSA-DES-CBC-SHA Kx=DH Au=RSA Enc=DES(56)
Mac=SHA1
DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56)
Mac=SHA1
TLSv1
EDH-RSA-DES-CBC-SHA Kx=DH Au=RSA Enc=DES(56)
Mac=SHA1
DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56)
Mac=SHA1

The fields above are :

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

Plugin ID:
42873

Backported Security Patch Detection (WWW)

Synopsis:
Security patches are
backported.

Description:
Security patches may have been
'back ported' to the remote HTTP server
without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any
security problem.

Risk factor:
None

See also:
http://www.nessus.org/u?d636c8c7

Solution:
N/A

Plugin output:
Give Nessus credentials to perform local checks.

Plugin ID:
39521

HTTP methods per directory

Synopsis:
This plugin determines
which HTTP methods are allowed on various CGI
directories.

Description:
By calling the OPTIONS
method, it is possible to determine which HTTP
methods are allowed on each directory.

As this list may be incomplete, the plugin also tests - if 'Thorough
tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and
considers them as unsupported if it receives a response code of 400,
403, 405, or 501.

Note that the plugin output is only informational and does not
necessarily indicate the presence of any security vulnerabilities.

**Risk
factor:**
None

Solution:
n/a

**Plugin
output:**
Based on the response to an OPTIONS request :

- HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

/

Plugin ID:
43111

HyperText Transfer Protocol (HTTP) Information

Synopsis:
Some information about the
remote HTTP configuration can be extracted.

Description:
This
test gives some information about the remote HTTP protocol - the
version used, whether HTTP Keep-Alive and HTTP pipelining are enabled,
etc...

This test is informational only and does not denote any security
problem.

Risk factor:
None

Solution:
n/a

**Plugin
output:**

Protocol version : HTTP/1.0
SSL : yes
Keep-Alive : no
Options allowed : GET,HEAD,POST,OPTIONS,TRACE
Headers :

Date: Fri, 14 May 2010 10:28:28 GMT
Server: Apache/2.0.52 (CentOS)
Accept-Ranges: bytes
Content-Length: 4251
Connection: close
Content-Type: text/html; charset=UTF-8

Plugin ID:
24260

HTTP Server type and version

Synopsis:
A web server is running on
the remote host.

Description:
This plugin attempts to
determine the type and the version of the
remote web server.

Risk factor:
None

Solution:
n/a

**Plugin
output:**
The remote web server type is :

Apache/2.0.52 (CentOS)

Solution : You can set the directive 'ServerTokens Prod' to limit
the information emanating from the server in its response headers.

**Plugin
ID:**
10107

SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection

Synopsis:
The remote service allows
renegotiation of TLS / SSL connections.

Description:
The
remote service encrypts traffic using TLS / SSL but allows a
client to renegotiate the connection after the initial handshake. An
unauthenticated remote attacker may be able to leverage this issue to
inject an arbitrary amount of plaintext into the beginning of the
application protocol stream, which could facilitate man-in-the-middle
attacks if the service assumes that the sessions before and after
renegotiation are from the same 'client' and merges them at the
application layer.

Risk factor:
Low

CVSS Base
Score:2.6
CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N

See also:
http://extendedsubset.com/?p=8

See
also:
http://www.ietf.org/mail-archive/web/tls/current/msg03948.html

See
also:
http://www.kb.cert.org/vuls/id/120541

See also:
http://www.g-sec.lu/practicaltls.pdf

See
also:
http://tools.ietf.org/html/rfc5746

Solution:
Contact
the vendor for specific patch information.

Plugin ID:
42880

CVE:

CVE-2009-3555

BID:
36935

Other
references:
OSVDB:59968, OSVDB:59969, OSVDB:59970, OSVDB:59971,
OSVDB:59972, OSVDB:59973, OSVDB:59974, OSVDB:60521, OSVDB:61234,
OSVDB:61718, OSVDB:62210, OSVDB:62536

SSL Cipher Suites Supported

Synopsis:
The remote service
encrypts communications using SSL.

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

Risk factor:
None

**See
also:**
http://www.openssl.org/docs/apps/ciphers.html

Solution:
n/a

**Plugin
output:**

Here is the list of 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-EDH-RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES(40)
Mac=SHA1 export
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-EDH-RSA-DES-CBC-SHA Kx=DH(512) Au=RSA Enc=DES(40)
Mac=SHA1 export
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

Medium Strength Ciphers (>= 56-bit and < 112-bit key)
SSLv2
DES-CBC-MD5 Kx=RSA Au=RSA Enc=DES(56)
Mac=MD5
RC4-64-MD5 Kx=RSA Au=RSA Enc=RC4(64)
Mac=MD5
SSLv3
EDH-RSA-DES-CBC-SHA Kx=DH Au=RSA Enc=DES(56)
Mac=SHA1
DES-CBC-SHA Kx=RSA Au=RSA Enc=DES(56)
Mac=SHA1
TLSv1
EDH-RSA-DES-CBC-SHA Kx=DH Au=RSA Enc=DES(56)
Mac=SHA1

SSL Certificate Signed using Weak Hashing Algorithm

Synopsis:
The SSL certificate has
been signed using a weak hash algorithm.

Description:
The
remote service uses an SSL certificate that has been signed using
a cryptographically weak hashing algorithm - MD2, MD4, or MD5. These
algorithms are known to be vulnerable to collision attacks. In
theory, a determined attacker may be able to leverage this weakness to
generate another certificate with the same digital signature, which
could allow him to masquerade as the affected service.

**Risk
factor:**
Low

CVSS Base Score:2.6
CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N

**See
also:**
http://tools.ietf.org/html/rfc3279

See also:
http://www.phreedom.org/research/rogue-ca/

**See
also:**
http://www.microsoft.com/technet/security/advisory/961509.mspx

**See
also:**
http://www.kb.cert.org/vuls/id/836068

Solution:
Contact
the Certificate Authority to have the certificate reissued.

**Plugin
ID:**
35291

CVE:

CVE-2004-2761

BID:
11849, 33065

**Other
references:**
OSVDB:45106, OSVDB:45108, OSVDB:45127

SSL Certificate Information

Synopsis:
This plugin displays the
SSL certificate.

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

Risk factor:
None

Solution:
n/a

Plugin output:
Subject Name:

Country: --
State/Province: SomeState
Locality: SomeCity
Organization: SomeOrganization
Organization Unit: SomeOrganizationalUnit
Common Name: localhost.localdomain
Email Address: root@localhost.localdomain

Issuer Name:

Country: --
State/Province: SomeState
Locality: SomeCity
Organization: SomeOrganization
Organization Unit: SomeOrganizationalUnit
Common Name: localhost.localdomain
Email Address: root@localhost.localdomain

Serial Number: 00

Version: 3

Signature Algorithm: MD5 With RSA Encryption

Not Valid Before: May 12 06:52:50 2010 GMT
Not Valid After: May 12 06:52:50 2011 GMT

Public Key Info:

Algorithm: RSA Encryption
Public Key: 00 CD A8 01 01 61 5D CC 03 4B C3 2C 9B A8 CC 6B CF 2A D1 9C
55 93 1B 63 52 D5 EC 7E 0B BD 8B 43 D9 58 6D 4A 79 AD 42 3D
A4 3E DC 1A 75 B0 FD D6 5A 8D 16 35 DF CE 11 8E D9 BC D9 2E
52 3E 7F 24 1A 80 27 58 C2 EC 3D 86 66 CC E5 57 F3 EC 76 FA
55 0B 51 38 CB A5 84 C9 D2 42 8C 5E C1 BC 25 BA 64 6B F9 EA
8B 9E 71 A8 DD 00 86 4F EF 97 32 82 0B F0 55 39 2D E2 B8 6A
34 FD 88 BC E8 ED B2 7A 55
Exponent: 01 00 01

Signature: 00 CA 2E 33 47 72 B6 16 31 2F 67 4F 22 70 F9 9E 33 35 BF DB
C0 EF 6E 45 50 3B 10 5D 0D 1D 7F DB 95 97 E8 03 0D C9 48 C1
BD 2F 3B BA 39 75 80 F1 8B 4B FB 70 CF B6 70 89 D6 07 53 B4
BC 41 AF 65 34 68 A8 0E BD 48 DF 90 CD E8 A7 BC 61 30 D0 8E
FD C4 99 44 90 5D AC 86 37 89 EC 48 5A E8 B8 38 BE 39 8A EC

Service Detection

A web server is running on this port through
SSLv2.

Plugin ID:
22964

Service Detection

An SSLv2 server answered on this port.

Plugin ID:
22964

Port www (631/tcp) [-/+]

HTTP methods per directory

Synopsis:
This plugin determines
which HTTP methods are allowed on various CGI
directories.

Description:
By calling the OPTIONS
method, it is possible to determine which HTTP
methods are allowed on each directory.

As this list may be incomplete, the plugin also tests - if 'Thorough
tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and
considers them as unsupported if it receives a response code of 400,
403, 405, or 501.

Note that the plugin output is only informational and does not
necessarily indicate the presence of any security vulnerabilities.

**Risk
factor:**
None

Solution:
n/a

**Plugin
output:**
Based on the response to an OPTIONS request :

- HTTP methods HEAD OPTIONS POST PUT GET are allowed on :

/

Plugin ID:
43111

HTTP Server type and version

Synopsis:
A web server is running on
the remote host.

Description:
This plugin attempts to
determine the type and the version of the
remote web server.

Risk factor:
None

Solution:
n/a

**Plugin
output:**
The remote web server type is :

CUPS/1.1

Plugin ID:
10107

Service Detection

A web server is running on this port.

**Plugin
ID:**
22964

Port www (80/tcp) [-/+]

Web Server Expect Header XSS

Synopsis:
The remote web server is
vulnerable to a cross-site scripting attack.

Description:
The
remote web server fails to sanitize the contents of an 'Expect'
request header before using it to generate dynamic web content. An
unauthenticated remote attacker may be able to leverage this issue to
launch cross-site scripting attacks against the affected service,
perhaps through specially-crafted ShockWave (SWF) files.

**Risk
factor:**
Medium

CVSS Base Score:4.3
CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N

**See
also:**
http://archives.neohapsis.com/archives/bugtraq/2006-05/0151.html

**See
also:**
http://archives.neohapsis.com/archives/bugtraq/2006-05/0441.html

**See
also:**
http://archives.neohapsis.com/archives/bugtraq/2006-07/0425.html

**See
also:**
http://www.apache.org/dist/httpd/CHANGES_2.2

**See
also:**
http://www.apache.org/dist/httpd/CHANGES_2.0

**See
also:**
http://www.apache.org/dist/httpd/CHANGES_1.3

**See
also:**
http://www-1.ibm.com/support/docview.wss?uid=swg1PK24631

**See
also:**
http://www-1.ibm.com/support/docview.wss?uid=swg24017314

Solution:
Check
with the vendor for an update to the web server. For Apache,
the issue is reportedly fixed by versions 1.3.35 / 2.0.57 / 2.2.2; for
IBM HTTP Server, upgrade to 6.0.2.13 / 6.1.0.1; for IBM WebSphere
Application Server, upgrade to 5.1.1.17.

Plugin output:

Nessus was able to exploit the issue using the following request :

---------- snip ----------
GET / HTTP/1.1

HTTP TRACE / TRACK Methods Allowed

Synopsis:
Debugging functions are
enabled on the remote web server.

Description:
The
remote webserver supports the TRACE and/or TRACK methods. TRACE
and TRACK are HTTP methods that are used to debug web server
connections.

Risk factor:
Medium

CVSS Base
Score:4.3
CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N

See also:
http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

See
also:
http://www.apacheweek.com/issues/03-01-24

See
also:
http://www.kb.cert.org/vuls/id/288308

See also:
http://www.kb.cert.org/vuls/id/867593

See
also:
http://sunsolve.sun.com/search/document.do?assetkey=1-66-200942-1

Solution:
Disable
these methods. Refer to the plugin output for more information.

Plugin
output:

To disable these methods, add the following lines for each virtual
host in your configuration file :

RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]

Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2
support disabling the TRACE method natively via the 'TraceEnable'
directive.

Nessus sent the following TRACE request :

---------- snip ----------
TRACE /Nessus842466213.html HTTP/1.1
Connection: Close
Host: 192.168.1.10
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1;
Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png,

Backported Security Patch Detection (WWW)

Synopsis:
Security patches are
backported.

Description:
Security patches may have been
'back ported' to the remote HTTP server
without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any
security problem.

Risk factor:
None

See also:
http://www.nessus.org/u?d636c8c7

Solution:
N/A

**Plugin
output:**
Give Nessus credentials to perform local checks.

**Plugin
ID:**
39521

HTTP methods per directory

Synopsis:
This plugin determines
which HTTP methods are allowed on various CGI
directories.

Description:
By calling the OPTIONS
method, it is possible to determine which HTTP
methods are allowed on each directory.

As this list may be incomplete, the plugin also tests - if 'Thorough
tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and
considers them as unsupported if it receives a response code of 400,
403, 405, or 501.

Note that the plugin output is only informational and does not
necessarily indicate the presence of any security vulnerabilities.

**Risk
factor:**
None

Solution:
n/a

**Plugin
output:**
Based on the response to an OPTIONS request :

- HTTP methods GET HEAD OPTIONS POST TRACE are allowed on :

/

Plugin ID:
43111

HyperText Transfer Protocol (HTTP) Information

Synopsis:
Some information about the
remote HTTP configuration can be extracted.

Description:
This
test gives some information about the remote HTTP protocol - the
version used, whether HTTP Keep-Alive and HTTP pipelining are enabled,
etc...

This test is informational only and does not denote any security
problem.

Risk factor:
None

Solution:
n/a

**Plugin
output:**

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : GET,HEAD,POST,OPTIONS,TRACE
Headers :

Date: Fri, 14 May 2010 10:28:28 GMT
Server: Apache/2.0.52 (CentOS)
Accept-Ranges: bytes
Content-Length: 4251
Connection: close
Content-Type: text/html; charset=UTF-8

Plugin ID:
24260

HTTP Server type and version

Synopsis:
A web server is running on
the remote host.

Description:
This plugin attempts to
determine the type and the version of the
remote web server.

Risk factor:
None

Solution:
n/a

**Plugin
output:**
The remote web server type is :

Apache/2.0.52 (CentOS)

Solution : You can set the directive 'ServerTokens Prod' to limit
the information emanating from the server in its response headers.

**Plugin
ID:**
10107

Service Detection

A web server is running on this port.

**Plugin
ID:**
22964

Port rpc-status (857/udp) [-/+]

RPC Services Enumeration

Synopsis:
An ONC RPC service is
running on the remote host.

Description:
By sending a
DUMP request to the portmapper, it was possible to
enumerate the ONC RPC services running on the remote port. Using this
information, it is possible to connect and bind to each service by
sending an RPC request to the remote port.

Risk factor:
None

Solution:
n/a

**Plugin
output:**

The following RPC services are available on UDP port 857 :

- program: 100024 (status), version: 1

Plugin ID:
11111

Port rpc-status (860/tcp) [-/+]

RPC Services Enumeration

Synopsis:
An ONC RPC service is
running on the remote host.

Description:
By sending a
DUMP request to the portmapper, it was possible to
enumerate the ONC RPC services running on the remote port. Using this
information, it is possible to connect and bind to each service by
sending an RPC request to the remote port.

Risk factor:
None

Solution:
n/a

**Plugin
output:**

The following RPC services are available on TCP port 860 :

- program: 100024 (status), version: 1

Plugin ID:
11111

[^] Back to 192.168.1.10