Nessus Report

Report

20/Feb/2013:08:24:15 GMT

HomeFeed: Commercial use of the report is prohibited

Table Of Contents

Hosts Summary (Executive)

amibaltoledo.es

Summary

Critical	High	Medium	Low	Info	Total
0	0	2	2	23	27

Details

Severity	Plugin Id	Name
Medium (5.0)	10079	Anonymous FTP Enabled
Medium (5.0)	46803	PHP expose_php Information Disclosure
Low (2.6)	26194	Web Server Uses Plain Text Authentication Forms
Low (2.6)	34324	FTP Supports Clear Text Authentication
Info	10092	FTP Server Detection
Info	10107	HTTP Server Type and Version
Info	10287	Traceroute Information
Info	10302	Web Server robots.txt Information Disclosure
Info	10662	Web mirroring
Info	11219	Nessus SYN scanner
Info	11419	Web Server Office File Inventory
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	18638	Drupal Software Detection
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	39463	HTTP Server Cookies Set
Info	39521	Backported Security Patch Detection (WWW)
Info	42057	Web Server Allows Password Auto-Completion
Info	45590	Common Platform Enumeration (CPE)
Info	46180	Additional DNS Hostnames
Info	49704	External URLs
Info	49705	Gathered e-mail Addresses
Info	54615	Device Type

Info	57323	OpenSSL Version Detection

Vulnerabilities By Host

amibaltoledo.es

Scan Information

Start time:	Tue Feb 19 08:17:18 2013
End time:	Wed Feb 20 08:24:11 2013

Host Information

DNS Name:	amibaltoledo.es
IP:	81.169.145.150
OS:	Microsoft Windows Vista

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	2	2	26	30

Results Details

0/tcp

12053 - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the FQDN of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/02/11, Modification date: 2012/09/28

Ports

tcp/0

```
81.169.145.150 resolves as amibaltoledo.es.
```

25220 - 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.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Ports

tcp/0

46180 - Additional DNS Hostnames

Synopsis

Potential virtual hosts have been detected.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Different web servers may be hosted on name- based virtual hosts.

See Also

http://en.wikipedia.org/wiki/Virtual_hosting

Solution

If you want to test them, re-scan using the special vhost syntax, such as :
www.example.com[192.0.32.10]

Risk Factor

None

Plugin Information:

Publication date: 2010/04/29, Modification date: 2013/01/21

Ports

tcp/0

```
The following hostnames point to the remote host:
  - www.amibaltoledo.es
```

11936 - OS Identification

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 Information:

Publication date: 2003/12/09, Modification date: 2012/12/01

Ports

tcp/0

```
Remote operating system : Microsoft Windows Vista
Confidence Level : 65
Method : SinFP


The remote host is running Microsoft Windows Vista
```

54615 - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Ports

tcp/0

```
Remote device type : general-purpose
Confidence level : 65
```

45590 - 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.

See Also

http://cpe.mitre.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2013/01/17

Ports

tcp/0

```
The remote operating system matched the following CPE :

  cpe:/o:microsoft:windows_vista

Following application CPE's matched on the remote system :

  cpe:/a:openssl:openssl:0.9.8r -> OpenSSL Project OpenSSL 0.9.8r
  cpe:/a:modssl:mod_ssl:2.2.21
  cpe:/a:apache:http_server:2.2.21 -> Apache HTTP Server 2.2.21
  cpe:/a:php:php:5.2.17 -> PHP 5.2.17
```

19506 - Nessus Scan Information

Synopsis

Information about the Nessus scan.

Description

This script displays, for each tested host, information about the scan itself :
- The version of the plugin set
- The type of plugin feed (HomeFeed or ProfessionalFeed)
- The version of the Nessus Engine
- The port scanner(s) used
- The port range scanned
- Whether credentialed or third-party patch management checks are possible
- The date of the scan
- The duration of the scan
- The number of hosts scanned in parallel
- The number of checks done in parallel

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2012/10/31

Ports

tcp/0

```
Information about this scan :

Nessus version : 5.0.2
Plugin feed version : 201302172115
Type of plugin feed : HomeFeed (Non-commercial use only)
Scanner IP : 10.138.93.220
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2013/2/19 8:17
Scan duration : 86809 sec
```

0/udp

10287 - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2011/03/21

Ports

udp/0

```
For your information, here is the traceroute from 10.138.93.220 to 81.169.145.150 :
10.138.93.220
10.138.64.2
81.169.145.150
```

21/tcp

10079 - Anonymous FTP Enabled

Synopsis

Anonymous logins are allowed on the remote FTP server.

Description

This FTP service allows anonymous logins. Any remote user may connect and authenticate without providing a password or unique credentials. This allows a user to access any files made available on the FTP server.

Solution

Disable anonymous FTP if it is not required. Routinely check the FTP server to ensure sensitive content is not available.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-1999-0497
XREF	OSVDB:69

Plugin Information:

Publication date: 1999/06/22, Modification date: 2013/01/25

Ports

tcp/21

34324 - FTP Supports Clear Text Authentication

Synopsis

Authentication credentials might be intercepted.

Description

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

Solution

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

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

XREF	CWE:522
XREF	CWE:523

Plugin Information:

Publication date: 2008/10/01, Modification date: 2013/01/25

Ports

tcp/21

```
This FTP server does not support 'AUTH TLS'.
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner.
It shall be reasonably quick even against a firewalled target.
Note that SYN scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Ports

tcp/21

```
Port 21/tcp was found to be open
```

10092 - FTP Server Detection

Synopsis

An FTP server is listening on this port.

Description

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

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2011/03/15

Ports

tcp/21

```
The remote FTP banner is :

220 Speak friend, and enter
```

80/tcp

46803 - PHP expose_php Information Disclosure

Synopsis

The configuration of PHP on the remote host allows disclosure of sensitive information.

Description

The PHP install on the remote server is configured in a way that allows disclosure of potentially sensitive information to an attacker through a special URL. Such a URL triggers an Easter egg built into PHP itself.
Other such Easter eggs likely exist, but Nessus has not checked for them.

See Also

http://www.0php.com/php_easter_egg.php

http://seclists.org/webappsec/2004/q4/324

Solution

In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

XREF OSVDB:12184

Plugin Information:

Publication date: 2010/06/03, Modification date: 2012/09/05

Ports

tcp/80

```
Nessus was able to verify the issue using the following URL :

  http://amibaltoledo.es/index.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
```

26194 - Web Server Uses Plain Text Authentication Forms

Synopsis

The remote web server might transmit credentials in cleartext.

Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.
An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Solution

Make sure that every sensitive form transmits content over HTTPS.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

XREF	CWE:522
XREF	CWE:523
XREF	CWE:718
XREF	CWE:724

Plugin Information:

Publication date: 2007/09/28, Modification date: 2011/09/15

Ports

tcp/80

```
Page : /
Destination page : /node?destination=node
Input name : pass


Page : /listado-de-noticias
Destination page : /listado-de-noticias?destination=listado-de-noticias
Input name : pass


Page : /qui%C3%A9nes-somos
Destination page : /qui%C3%A9nes-somos?destination=node/2
Input name : pass


Page : /404
Destination page : /404?destination=node/50
Input name : pass


Page : /lista-de-jugadores/3
Destination page : /lista-de-jugadores/3?destination=lista-de-jugadores/3
Input name : pass


Page : /lista-de-jugadores/4
Destination page : /lista-de-jugadores/4?destination=lista-de-jugadores/4
Input name : pass


Page : /lista-de-jugadores/5
Destination page : /lista-de-jugadores/5?destination=lista-de-jugadores/5
Input name : pass


Page : /lista-de-jugadores/6
Destination page : /lista-de-jugadores/6?destination=lista-de-jugadores/6
Input name : pass
```

```
Page : /lista-de-jugadores/7
Destination page : /lista-de-jugadores/7?destination=lista-de-jugadores/7
Input name : pass


Page : /lista-de-jugadores/8
Destination page : /lista-de-jugadores/8?destination=lista-de-jugadores/8
Input name : pass


Page : /lista-de-jugadores/9
Destination page : /lista-de-jugadores/9?destination=lista-de-jugadores/9
Input name : pass


Page : /listado-de-tecnicos
Destination page : /listado-de-tecnicos?destination=listado-de-tecnicos
Input name : pass


Page : /403
Destination page : /403?destination=node/51
Input name : pass


Page : /gallery-collections/galer%C3%AD
Destination page : /gallery-collections/galer%C3%AD?destination=taxonomy/term/17
Input name : pass


Page : /listado-de-patocinadores
Destination page : /listado-de-patocinadores?destination=listado-de-patocinadores
Input name : pass


Page : /contact
Destination page : /contact?destination=contact
Input name : pass


Page : /inscripcion
Destination page : /inscripcion?destination=node/63
Input name : pass


Page : /el-gobierno-municipal-muestra-su-apoyo-al-balonmano-toledano
Destination page : /el-gobierno-municipal-muestra-su-apoyo-al-balonmano-toledano?
destination=node/1 [...]
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner.
It shall be reasonably quick even against a firewalled target.
Note that SYN scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Ports

tcp/80

```
Port 80/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2013/02/15

Ports

tcp/80

```
A web server is running on this port.
```

10662 - Web mirroring

Synopsis

Nessus crawled the remote web site.

Description

This script makes a mirror of the remote web site(s) and extracts the list of CGIs that are used by the remote host.
It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/05/04, Modification date: 2012/01/04

Ports

tcp/80

```
The following CGI have been discovered :

Syntax : cginame (arguments [default value])

/media-gallery/detail/110/142 (form_build_id [form-52xL2GrI9jUOP1gqdPGneTasUqAHZptluXCipLDA4pM]
 openi...)
/node/67 (search_block_form [] op [Buscar] form_build_id [form-nXCgqCw3lERJS8mra...)
/media-gallery/detail/27/31 (form_build_id [form-UZ2UfCPiatmo9LcOfUWhvKZO7-HDTX_1UPFSywdliAE]
 openi...)
/modules/openid/openid.js (mibbos [] )
/media-gallery/detail/111/158 (form_build_id [form-swx5fJng0ghL_OlDT-Pzrr9z3nkD1rjIDSFcysGPS4g]
 openi...)
/misc/form.js (v [7.17] )
/%C2%BFes-necesario-reforzar-la-plantilla-del-primer-equipo (form_build_id [form-
dCOznTtQl_8wLor7BwpZYcwKoigx3dNjBEXbFkKEF-c] openi...)
/sites/all/modules/simpleads/simpleads.js (mibbos [] )
/torneo-ciudad-c%C3%B3rdoba (form_build_id [form-X96CFrOG33mQ-KzBeTNPBe4bJI3voiriTvg9tCk7hOU]
 openi...)
/listado-de-patocinadores (form_build_id [form-Yt_qm2Q3D7VJuIFxYPdXeSqD1uxiCAqup7MqiazZA14]
 openi...)
/taxonomy/term/17 (search_block_form [] op [Buscar] form_build_id [form-hjbB0n8rgtawdwU5o...)
/node/64 (search_block_form [] op [Buscar] form_build_id [form-TDDlNCTWc_aSL15T7...)
/node/139 (search_block_form [] op [Buscar] form_build_id [form-lExzHNmhJjxRoZ1uN...)
/sites/all/modules/nice_menus/superfish/js/jquery.bgiframe.min.js (mibbos [] )
/node/89 (search_block_form [] op [Buscar] form_build_id [form-bq8oZklpza9CK8Mt5...)
/media-gallery/detail/27/30 (form_build_id [form-lzQeCqTJXFPi9zW94AQSmi13u9qyj3v0IAE5Zk6JM9w]
 openi...)
/media-gallery/detail/27/25 (form_build_id [form--1mbic0DLSxwRWik5khDFMI_glsJdm2yrg3OdfMPc-E]
 openi...)
```

```
/formulario-inscripci%C3%B3n-y-autorizaciones (details[sid] [] destination [node/60] form_build_id
 [form-wtZZRoWU6tBL...)
/sites/all/modules/webform/js/webform.js (mibbos [] )
/contact (form_build_id [form-RHb3L3UmtsHyebbngaeJYnA4PrCRQLaqz6h4mZw_K_k] openi...)
/media-gallery/detail/111/176 (form_build_id [form-5JUjLmtS6jr4MqqWh8te4-OiOYN5dspS_3AnBIRnwTE]
 openi...)
/media-gallery/detail/110/128 (form_build_id [form-u79IIBPbGZD0S4ywEo2T8rs6cXsyFlR2L4sRObUyhI
 [...]
```

49705 - Gathered e-mail Addresses

Synopsis

e-mail addresses were gathered.

Description

Nessus gathered mailto: HREF links and extracted e-mail addresses by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/10/04, Modification date: 2011/03/18

Ports

tcp/80

```
The following email address has been gathered :


- 'cdamibaltoledo@gmail.com', referenced from :
   /c%C3%B3mo-apuntarse-al-club-sin-moverse-casa
   /node/63
   /node/64
   /listado-de-patocinadores
   /inscripcion
```

42057 - Web Server Allows Password Auto-Completion

Synopsis

Auto-complete is not disabled on password fields.

Description

The remote web server contains at least HTML form field containing an input of type 'password' where 'autocomplete' is not set to 'off'.
While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or their machine is compromised at some point.

Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

Risk Factor

None

Plugin Information:

Publication date: 2009/10/07, Modification date: 2011/09/28

Ports

tcp/80

```
Page : /
Destination Page : /node?destination=node
Input name : pass



Page : /listado-de-noticias
```

```
Destination Page : /listado-de-noticias?destination=listado-de-noticias
Input name : pass



Page : /qui%C3%A9nes-somos
Destination Page : /qui%C3%A9nes-somos?destination=node/2
Input name : pass



Page : /404
Destination Page : /404?destination=node/50
Input name : pass



Page : /lista-de-jugadores/3
Destination Page : /lista-de-jugadores/3?destination=lista-de-jugadores/
3
Input name : pass



Page : /lista-de-jugadores/4
Destination Page : /lista-de-jugadores/4?destination=lista-de-jugadores/
4
Input name : pass



Page : /lista-de-jugadores/5
Destination Page : /lista-de-jugadores/5?destination=lista-de-jugadores/
5
Input name : pass



Page : /lista-de-jugadores/6
Destination Page : /lista-de-jugadores/6?destination=lista-de-jugadores/
6
Input name : pass



Page : /lista-de-jugadores/7
Destination Page : /lista-de-jugadores/7?destination=lista-de-jugadores/
7
Input name : pass



Page : /lista-de-jugadores/8
Destination Page : /lista-de-jugadores/8?destination=lista-de-jugadores/
8
Input name : pass



Page : /lista-de-jugadores/9
Destination Page : /lista-de-jugadores/9?destination=lista-de-jugadores/
9
Input name : pass
```

```
Page : /listado-de-tecnicos
Destination Page : /listado-de-tecnicos?destination=listado-de-tecnicos
Input name : pass



Page : /403
Destination Page : /403?destination=node/51
Input name : pass



Page : /gallery-collections/galer%C3%AD
Destination Page : /gallery-collections/galer%C3%AD?destination=taxonomy
/term/17
Input name : pass



Page : /listado-de-patocinadores
Destination Page : /listado-de-patocinadores?destination=listado-de-pato
cinadores
Input name : pass



Page : /contact
Destination Page : /contact?destination=contact
Input name : pass



Page : /inscripcion
Destination Page : /inscripcion?destination=node/63
Input name : pass



Page : /el-gobierno-municipal-muestra-su-apoyo-al-balonmano-toledano
Destination Page : /el-gobierno-municipal-muestra-su-apo [...]
```

49704 - External URLs

Synopsis

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/10/04, Modification date: 2011/08/19

Ports

tcp/80

```
25 external URLs were gathered on this web server :
URL...                                  - Seen on...

http://11/02/2013                       - /listado-de-patocinadores

http://AMIAB                            - /listado-de-patocinadores
```

```
http://Ergonalia                        - /listado-de-patocinadores
http://Lozoya                           - /listado-de-patocinadores
http://Previcaman                       - /listado-de-patocinadores
http://aqs                              - /listado-de-patocinadores
http://fitness                          - /listado-de-patocinadores
http://openid.net/                      - /
http://portal.lacaixa.es/home/particulares_es.html - /listado-de-patocinadores
http://www.alquiler-autocares.es/       - /listado-de-patocinadores
http://www.alvarezmartin.com/           - /listado-de-patocinadores
http://www.amibaltoledo.es              - /inauguracion-pagina-web
http://www.ayto-toledo.org              - /listado-de-patocinadores
http://www.clm24.es/articulo/deportes/el-gobierno-municipal-muestra-su-apoyo-al-balonmano-
toledano/20130217114612002951.html - /el-gobierno-municipal-muestra-su-apoyo-al-balonmano-toledano
http://www.diputoledo.es/               - /listado-de-patocinadores
http://www.fbmclm.com/competiciones.asp?v=18&torneo=175 - /
http://www.fbmclm.com/competiciones.asp?v=18&torneo=184 - /
http://www.fbmclm.com/competiciones.asp?v=18&torneo=185 - /
http://www.latribunadetoledo.es/        - /amibal-se-reinventa-para-garantizar-el-futuro
http://www.latribunadetoledo.es/noticia/Z201446B1-9618-95C5-EEDE75A4D68EB1BD/20130203/alvaro/
guimare/anota/in/extremis/amibal/regresa/victoria - /etiquetas/resultados
http://www.latribunadetoledo.es/noticia/ZEDC49721-E4C8-8DB7-1D9C4331BB3E2DA1/20130217/tarde/
tranquila - /
http://www.ortopediatoledo.com/         - /listado-de-patocinadores
http://www.pentatel.es/                 - /listado-de-patocinadores
http://www.rfebm.net/competiciones.asp?v=18&torneo=2899 - /
http://www.youtube.com/embed/DVzdLnUd0-c?wmode=opaque - /no-perdamos-nuestr [...]
```

39463 - HTTP Server Cookies Set

Synopsis

Some cookies have been set by the web server.

Description

HTTP cookies are pieces of information that are presented by web servers and are sent back by the browser.
As HTTP is a stateless protocol, cookies are a possible mechanism to keep track of sessions.
This plugin displays the list of the HTTP cookies that were set by the web server when it was crawled.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/06/19, Modification date: 2011/03/15

Ports

tcp/80

```
domain   = .amibaltoledo.es
path     = /
name     = SESS1451a2cb2d2acfc158a3c130ff75da65
value    = deleted
version  = 1
expires  = Mon, 20-Feb-2012 07:33:14 GMT
secure   = 0
httponly = 1
```

10107 - 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.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/01/04, Modification date: 2012/08/02

Ports
tcp/80

```
The remote web server type is :

Apache/2.2.21 (Unix) mod_ssl/2.2.21 OpenSSL/0.9.8r

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

24260 - 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.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/01/30, Modification date: 2011/05/31

Ports
tcp/80

```
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Tue, 19 Feb 2013 07:40:59 GMT
  Server: Apache/2.2.21 (Unix) mod_ssl/2.2.21 OpenSSL/0.9.8r
  X-Powered-By: PHP/5.2.17
  Expires: Sun, 19 Nov 1978 05:00:00 GMT
  Cache-Control: no-cache, must-revalidate, post-check=0, pre-check=0
  ETag: "1361259659"
  Content-Language: es
  X-Generator: Drupal 7 (http://drupal.org)
  Link: <http://amibaltoledo.es/>; rel="canonical",<http://amibaltoledo.es/>; rel="shortlink"
  Keep-Alive: timeout=3, max=72
  Content-Type: text/html; charset=utf-8
  Transfer-Encoding: chunked
  Last-Modified: Tue, 19 Feb 2013 07:40:59 UTC
  Connection: keep-alive
```

57323 - OpenSSL Version Detection

Synopsis

The version of OpenSSL can be identified.

Description

The version of OpenSSL could be extracted from the web server's banner. Note that in many cases, security patches are backported and the displayed version number does not show the patch level. Using it to identify vulnerable software is likely to lead to false detections.

See Also

http://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/16, Modification date: 2011/12/16

Ports

tcp/80

```
Source                : Server: Apache/2.2.21 (Unix) mod_ssl/2.2.21 OpenSSL/0.9.8r
Version (from banner) : 0.9.8r
```

18638 - Drupal Software Detection

Synopsis

The remote web server contains a content management system written in PHP.

Description

The remote host is running Drupal, an open source content management system written in PHP.

See Also

http://drupal.org/

Solution

Make sure the use of this program is in accordance with your corporate security policy.

Risk Factor

None

Plugin Information:

Publication date: 2005/07/07, Modification date: 2013/01/22

Ports

tcp/80

```
The following instance of Drupal was detected on the remote host :

  Version : 7.17
  URL     : http://amibaltoledo.es/
```

11419 - Web Server Office File Inventory

Synopsis

The remote web server hosts office-related files.

Description

This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

Solution

Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

Risk Factor

None

Plugin Information:

Publication date: 2003/03/19, Modification date: 2011/12/28

Ports

tcp/80

```
The following office-related files are available on the remote server :

  - Adobe Acrobat files (.pdf) :
    /sites/default/files/documentos/ficha_inscripcion_autorizaciones.pdf
```

10302 - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a web site for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/wc/exclusion.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

References

XREF OSVDB:238

Plugin Information:

Publication date: 1999/10/12, Modification date: 2011/03/14

Ports

tcp/80

```
Contents of robots.txt :

#
# robots.txt
#
# This file is to prevent the crawling and indexing of certain parts
# of your site by web crawlers and spiders run by sites like Yahoo!
# and Google. By telling these "robots" where not to go on your site,
# you save bandwidth and server resources.
#
# This file will be ignored unless it is at the root of your host:
# Used:    http://example.com/robots.txt
# Ignored: http://example.com/site/robots.txt
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/wc/robots.html
#
# For syntax checking, see:
# http://www.sxw.org.uk/computing/robots/check.html

User-agent: *
Crawl-delay: 10
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /INSTALL.sqlite.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
```

```
Disallow: /filter/tips/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
Disallow: /user/logout/
# Paths (no clean URLs)
Disallow: /?q=admin/
Disallow: /?q=comment/reply/
Disallow: /?q=filter/tips/
Disallow: /?q=node/add/
Disallow: /?q=search/
Disallow: /?q=user/password/
Disallow: /?q=user/register/
Disallow: /?q=user/login/
Disallow: /?q=user/logout/
```

39521 - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' 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.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/06/25, Modification date: 2013/01/18

Ports

tcp/80

```
Give Nessus credentials to perform local checks.
```

443/tcp

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner.
It shall be reasonably quick even against a firewalled target.
Note that SYN scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Ports

tcp/443

```
Port 443/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2013/02/15

Ports

tcp/443

```
The service closed the connection without sending any data.
It might be protected by some sort of TCP wrapper.
```

Vulnerabilities By Plugin

10079 (1) - Anonymous FTP Enabled

Synopsis

Anonymous logins are allowed on the remote FTP server.

Description

This FTP service allows anonymous logins. Any remote user may connect and authenticate without providing a password or unique credentials. This allows a user to access any files made available on the FTP server.

Solution

Disable anonymous FTP if it is not required. Routinely check the FTP server to ensure sensitive content is not available.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

CVE	CVE-1999-0497
XREF	OSVDB:69

Plugin Information:

Publication date: 1999/06/22, Modification date: 2013/01/25

Hosts

amibaltoledo.es (tcp/21)

46803 (1) - PHP expose_php Information Disclosure

Synopsis

The configuration of PHP on the remote host allows disclosure of sensitive information.

Description

The PHP install on the remote server is configured in a way that allows disclosure of potentially sensitive information to an attacker through a special URL. Such a URL triggers an Easter egg built into PHP itself.
Other such Easter eggs likely exist, but Nessus has not checked for them.

See Also

http://www.0php.com/php_easter_egg.php

http://seclists.org/webappsec/2004/q4/324

Solution

In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

References

XREF OSVDB:12184

Plugin Information:

Publication date: 2010/06/03, Modification date: 2012/09/05

Hosts

amibaltoledo.es (tcp/80)

```
Nessus was able to verify the issue using the following URL :

  http://amibaltoledo.es/index.php/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
```

26194 (1) - Web Server Uses Plain Text Authentication Forms

Synopsis

The remote web server might transmit credentials in cleartext.

Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext.
An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users.

Solution

Make sure that every sensitive form transmits content over HTTPS.

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

XREF	CWE:522
XREF	CWE:523
XREF	CWE:718
XREF	CWE:724

Plugin Information:

Publication date: 2007/09/28, Modification date: 2011/09/15

Hosts

amibaltoledo.es (tcp/80)

```
Page : /
Destination page : /node?destination=node
Input name : pass


Page : /listado-de-noticias
Destination page : /listado-de-noticias?destination=listado-de-noticias
Input name : pass


Page : /qui%C3%A9nes-somos
Destination page : /qui%C3%A9nes-somos?destination=node/2
Input name : pass


Page : /404
Destination page : /404?destination=node/50
Input name : pass


Page : /lista-de-jugadores/3
Destination page : /lista-de-jugadores/3?destination=lista-de-jugadores/3
Input name : pass


Page : /lista-de-jugadores/4
Destination page : /lista-de-jugadores/4?destination=lista-de-jugadores/4
Input name : pass


Page : /lista-de-jugadores/5
Destination page : /lista-de-jugadores/5?destination=lista-de-jugadores/5
Input name : pass
```

```
Page : /lista-de-jugadores/6
Destination page : /lista-de-jugadores/6?destination=lista-de-jugadores/6
Input name : pass


Page : /lista-de-jugadores/7
Destination page : /lista-de-jugadores/7?destination=lista-de-jugadores/7
Input name : pass


Page : /lista-de-jugadores/8
Destination page : /lista-de-jugadores/8?destination=lista-de-jugadores/8
Input name : pass


Page : /lista-de-jugadores/9
Destination page : /lista-de-jugadores/9?destination=lista-de-jugadores/9
Input name : pass


Page : /listado-de-tecnicos
Destination page : /listado-de-tecnicos?destination=listado-de-tecnicos
Input name : pass


Page : /403
Destination page : /403?destination=node/51
Input name : pass


Page : /gallery-collections/galer%C3%AD
Destination page : /gallery-collections/galer%C3%AD?destination=taxonomy/term/17
Input name : pass


Page : /listado-de-patocinadores
Destination page : /listado-de-patocinadores?destination=listado-de-patocinadores
Input name : pass


Page : /contact
Destination page : /contact?destination=contact
Input name : pass


Page : /inscripcion
Destination page : /inscripcion?destination=node/63
Input name : pass


Page : /el-gobierno-municipal-muestra-su-apoyo-al-balonmano-toledano
Destination page : /el-gobierno-municipal-muestra-su-apoyo-al-balonmano-toledano?
destination=node/1 [...]
```

34324 (1) - FTP Supports Clear Text Authentication

Synopsis

Authentication credentials might be intercepted.

Description

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

Solution

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

Risk Factor

Low

CVSS Base Score

2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

References

XREF	CWE:522
XREF	CWE:523

Plugin Information:

Publication date: 2008/10/01, Modification date: 2013/01/25

Hosts

amibaltoledo.es (tcp/21)

```
This FTP server does not support 'AUTH TLS'.
```

11219 (3) - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner.
It shall be reasonably quick even against a firewalled target.
Note that SYN scanners are less intrusive than TCP (full connect) scanners against broken services, but they might kill lame misconfigured firewalls. They might also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Hosts

amibaltoledo.es (tcp/21)

```
Port 21/tcp was found to be open
```

amibaltoledo.es (tcp/80)

```
Port 80/tcp was found to be open
```

amibaltoledo.es (tcp/443)

```
Port 443/tcp was found to be open
```

22964 (2) - Service Detection

Synopsis

The remote service could be identified.

Description

It was possible to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/08/19, Modification date: 2013/02/15

Hosts

amibaltoledo.es (tcp/80)

```
A web server is running on this port.
```

amibaltoledo.es (tcp/443)

```
The service closed the connection without sending any data.
It might be protected by some sort of TCP wrapper.
```

10092 (1) - FTP Server Detection

Synopsis

An FTP server is listening on this port.

Description

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

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2011/03/15

Hosts

amibaltoledo.es (tcp/21)

```
The remote FTP banner is :

220 Speak friend, and enter
```

10107 (1) - 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.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/01/04, Modification date: 2012/08/02

Hosts

amibaltoledo.es (tcp/80)

```
The remote web server type is :

Apache/2.2.21 (Unix) mod_ssl/2.2.21 OpenSSL/0.9.8r

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

10287 (1) - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/11/27, Modification date: 2011/03/21

Hosts

amibaltoledo.es (udp/0)

```
For your information, here is the traceroute from 10.138.93.220 to 81.169.145.150 :
10.138.93.220
10.138.64.2
81.169.145.150
```

10302 (1) - Web Server robots.txt Information Disclosure

Synopsis

The remote web server contains a 'robots.txt' file.

Description

The remote host contains a file named 'robots.txt' that is intended to prevent web 'robots' from visiting certain directories in a web site for maintenance or indexing purposes. A malicious user may also be able to use the contents of this file to learn of sensitive documents or directories on the affected site and either retrieve them directly or target them for other attacks.

See Also

http://www.robotstxt.org/wc/exclusion.html

Solution

Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.

Risk Factor

None

References

XREF OSVDB:238

Plugin Information:

Publication date: 1999/10/12, Modification date: 2011/03/14

Hosts

amibaltoledo.es (tcp/80)

```
Contents of robots.txt :

#
# robots.txt
#
# This file is to prevent the crawling and indexing of certain parts
# of your site by web crawlers and spiders run by sites like Yahoo!
# and Google. By telling these "robots" where not to go on your site,
# you save bandwidth and server resources.
#
# This file will be ignored unless it is at the root of your host:
# Used:    http://example.com/robots.txt
# Ignored: http://example.com/site/robots.txt
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/wc/robots.html
#
# For syntax checking, see:
# http://www.sxw.org.uk/computing/robots/check.html

User-agent: *
Crawl-delay: 10
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /INSTALL.sqlite.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
```

```
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
Disallow: /user/logout/
# Paths (no clean URLs)
Disallow: /?q=admin/
Disallow: /?q=comment/reply/
Disallow: /?q=filter/tips/
Disallow: /?q=node/add/
Disallow: /?q=search/
Disallow: /?q=user/password/
Disallow: /?q=user/register/
Disallow: /?q=user/login/
Disallow: /?q=user/logout/
```

10662 (1) - Web mirroring

Synopsis

Nessus crawled the remote web site.

Description

This script makes a mirror of the remote web site(s) and extracts the list of CGIs that are used by the remote host.
It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/05/04, Modification date: 2012/01/04

Hosts

amibaltoledo.es (tcp/80)

```
The following CGI have been discovered :

Syntax : cginame (arguments [default value])

/media-gallery/detail/110/142 (form_build_id [form-52xL2GrI9jUOP1gqdPGneTasUqAHZptluXCipLDA4pM]
 openi...)
/node/67 (search_block_form [] op [Buscar] form_build_id [form-nXCgqCw3lERJS8mra...)
/media-gallery/detail/27/31 (form_build_id [form-UZ2UfCPiatmo9LcOfUWhvKZO7-HDTX_1UPFSywdliAE]
 openi...)
/modules/openid/openid.js (mibbos [] )
/media-gallery/detail/111/158 (form_build_id [form-swx5fJng0ghL_OlDT-Pzrr9z3nkD1rjIDSFcysGPS4g]
 openi...)
/misc/form.js (v [7.17] )
/%C2%BFes-necesario-reforzar-la-plantilla-del-primer-equipo (form_build_id [form-
dCOznTtQl_8wLor7BwpZYcwKoigx3dNjBEXbFkKEF-c] openi...)
/sites/all/modules/simpleads/simpleads.js (mibbos [] )
/torneo-ciudad-c%C3%B3rdoba (form_build_id [form-X96CFrOG33mQ-KzBeTNPBe4bJI3voiriTvg9tCk7hOU]
 openi...)
/listado-de-patocinadores (form_build_id [form-Yt_qm2Q3D7VJuIFxYPdXeSqD1uxiCAqup7MqiazZA14]
 openi...)
/taxonomy/term/17 (search_block_form [] op [Buscar] form_build_id [form-hjbB0n8rgtawdwU5o...)
/node/64 (search_block_form [] op [Buscar] form_build_id [form-TDDlNCTWc_aSL15T7...)
/node/139 (search_block_form [] op [Buscar] form_build_id [form-lExzHNmhJjxRoZ1uN...)
/sites/all/modules/nice_menus/superfish/js/jquery.bgiframe.min.js (mibbos [] )
/node/89 (search_block_form [] op [Buscar] form_build_id [form-bq8oZklpza9CK8Mt5...)
/media-gallery/detail/27/30 (form_build_id [form-lzQeCqTJXFPi9zW94AQSmi13u9qyj3v0IAE5Zk6JM9w]
 openi...)
/media-gallery/detail/27/25 (form_build_id [form--1mbic0DLSxwRWik5khDFMI_glsJdm2yrg3OdfMPc-E]
 openi...)
/formulario-inscripci%C3%B3n-y-autorizaciones (details[sid] [] destination [node/60] form_build_id
 [form-wtZZRoWU6tBL...)
/sites/all/modules/webform/js/webform.js (mibbos [] )
/contact (form_build_id [form-RHb3L3UmtsHyebbngaeJYnA4PrCRQLaqz6h4mZw_K_k] openi...)
/media-gallery/detail/111/176 (form_build_id [form-5JUjLmtS6jr4MqqWh8te4-OiOYN5dspS_3AnBIRnwTE]
 openi...)
/media-gallery/detail/110/128 (form_build_id [form-u79IIBPbGZD0S4ywEo2T8rs6cXsyFlR2L4sRObUyhI
 [...]
```

11419 (1) - Web Server Office File Inventory

Synopsis

The remote web server hosts office-related files.

Description

This plugin connects to the remote web server and attempts to find office-related files such as .doc, .ppt, .xls, .pdf etc.

Solution

Make sure that such files do not contain any confidential or otherwise sensitive information and that they are only accessible to those with valid credentials.

Risk Factor

None

Plugin Information:

Publication date: 2003/03/19, Modification date: 2011/12/28

Hosts

amibaltoledo.es (tcp/80)

```
The following office-related files are available on the remote server :

  - Adobe Acrobat files (.pdf) :
    /sites/default/files/documentos/ficha_inscripcion_autorizaciones.pdf
```

11936 (1) - OS Identification

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 Information:

Publication date: 2003/12/09, Modification date: 2012/12/01

Hosts

amibaltoledo.es (tcp/0)

```
Remote operating system : Microsoft Windows Vista
Confidence Level : 65
Method : SinFP


The remote host is running Microsoft Windows Vista
```

12053 (1) - Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the FQDN of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/02/11, Modification date: 2012/09/28

Hosts

amibaltoledo.es (tcp/0)

```
81.169.145.150 resolves as amibaltoledo.es.
```

18638 (1) - Drupal Software Detection

Synopsis

The remote web server contains a content management system written in PHP.

Description

The remote host is running Drupal, an open source content management system written in PHP.

See Also

http://drupal.org/

Solution

Make sure the use of this program is in accordance with your corporate security policy.

Risk Factor

None

Plugin Information:

Publication date: 2005/07/07, Modification date: 2013/01/22

Hosts

amibaltoledo.es (tcp/80)

```
The following instance of Drupal was detected on the remote host :

  Version : 7.17
  URL     : http://amibaltoledo.es/
```

19506 (1) - Nessus Scan Information

Synopsis

Information about the Nessus scan.

Description

This script displays, for each tested host, information about the scan itself :
- The version of the plugin set
- The type of plugin feed (HomeFeed or ProfessionalFeed)
- The version of the Nessus Engine
- The port scanner(s) used
- The port range scanned
- Whether credentialed or third-party patch management checks are possible
- The date of the scan
- The duration of the scan
- The number of hosts scanned in parallel
- The number of checks done in parallel

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2012/10/31

Hosts

amibaltoledo.es (tcp/0)

```
Information about this scan :

Nessus version : 5.0.2
Plugin feed version : 201302172115
Type of plugin feed : HomeFeed (Non-commercial use only)
Scanner IP : 10.138.93.220
Port scanner(s) : nessus_syn_scanner
Port range : 1-65535
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : enabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2013/2/19 8:17
Scan duration : 86809 sec
```

24260 (1) - 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.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/01/30, Modification date: 2011/05/31

Hosts

amibaltoledo.es (tcp/80)

```
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Tue, 19 Feb 2013 07:40:59 GMT
  Server: Apache/2.2.21 (Unix) mod_ssl/2.2.21 OpenSSL/0.9.8r
  X-Powered-By: PHP/5.2.17
  Expires: Sun, 19 Nov 1978 05:00:00 GMT
  Cache-Control: no-cache, must-revalidate, post-check=0, pre-check=0
  ETag: "1361259659"
  Content-Language: es
  X-Generator: Drupal 7 (http://drupal.org)
  Link: <http://amibaltoledo.es/>; rel="canonical",<http://amibaltoledo.es/>; rel="shortlink"
  Keep-Alive: timeout=3, max=72
  Content-Type: text/html; charset=utf-8
  Transfer-Encoding: chunked
  Last-Modified: Tue, 19 Feb 2013 07:40:59 UTC
  Connection: keep-alive
```

25220 (1) - 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.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2011/03/20

Hosts

amibaltoledo.es (tcp/0)

39463 (1) - HTTP Server Cookies Set

Synopsis

Some cookies have been set by the web server.

Description

HTTP cookies are pieces of information that are presented by web servers and are sent back by the browser.
As HTTP is a stateless protocol, cookies are a possible mechanism to keep track of sessions.
This plugin displays the list of the HTTP cookies that were set by the web server when it was crawled.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/06/19, Modification date: 2011/03/15

Hosts

amibaltoledo.es (tcp/80)

```
domain   = .amibaltoledo.es
path     = /
name     = SESS1451a2cb2d2acfc158a3c130ff75da65
value    = deleted
version  = 1
expires  = Mon, 20-Feb-2012 07:33:14 GMT
secure   = 0
httponly = 1
```

39521 (1) - Backported Security Patch Detection (WWW)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' 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.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/06/25, Modification date: 2013/01/18

Hosts

amibaltoledo.es (tcp/80)

```
Give Nessus credentials to perform local checks.
```

42057 (1) - Web Server Allows Password Auto-Completion

Synopsis

Auto-complete is not disabled on password fields.

Description

The remote web server contains at least HTML form field containing an input of type 'password' where 'autocomplete' is not set to 'off'.
While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or their machine is compromised at some point.

Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

Risk Factor

None

Plugin Information:

Publication date: 2009/10/07, Modification date: 2011/09/28

Hosts

amibaltoledo.es (tcp/80)

```
Page : /
Destination Page : /node?destination=node
Input name : pass



Page : /listado-de-noticias
Destination Page : /listado-de-noticias?destination=listado-de-noticias
Input name : pass



Page : /qui%C3%A9nes-somos
Destination Page : /qui%C3%A9nes-somos?destination=node/2
Input name : pass



Page : /404
Destination Page : /404?destination=node/50
Input name : pass



Page : /lista-de-jugadores/3
Destination Page : /lista-de-jugadores/3?destination=lista-de-jugadores/
3
Input name : pass



Page : /lista-de-jugadores/4
Destination Page : /lista-de-jugadores/4?destination=lista-de-jugadores/
4
Input name : pass



Page : /lista-de-jugadores/5
Destination Page : /lista-de-jugadores/5?destination=lista-de-jugadores/
5
```

```
Input name : pass



Page : /lista-de-jugadores/6
Destination Page : /lista-de-jugadores/6?destination=lista-de-jugadores/
6
Input name : pass



Page : /lista-de-jugadores/7
Destination Page : /lista-de-jugadores/7?destination=lista-de-jugadores/
7
Input name : pass



Page : /lista-de-jugadores/8
Destination Page : /lista-de-jugadores/8?destination=lista-de-jugadores/
8
Input name : pass



Page : /lista-de-jugadores/9
Destination Page : /lista-de-jugadores/9?destination=lista-de-jugadores/
9
Input name : pass



Page : /listado-de-tecnicos
Destination Page : /listado-de-tecnicos?destination=listado-de-tecnicos
Input name : pass



Page : /403
Destination Page : /403?destination=node/51
Input name : pass



Page : /gallery-collections/galer%C3%AD
Destination Page : /gallery-collections/galer%C3%AD?destination=taxonomy
/term/17
Input name : pass



Page : /listado-de-patocinadores
Destination Page : /listado-de-patocinadores?destination=listado-de-pato
cinadores
Input name : pass



Page : /contact
Destination Page : /contact?destination=contact
Input name : pass



Page : /inscripcion
```

```
Destination Page : /inscripcion?destination=node/63
Input name : pass



Page : /el-gobierno-municipal-muestra-su-apoyo-al-balonmano-toledano
Destination Page : /el-gobierno-municipal-muestra-su-apo [...]
```

45590 (1) - 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.

See Also

http://cpe.mitre.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2013/01/17

Hosts

amibaltoledo.es (tcp/0)

```
The remote operating system matched the following CPE :

  cpe:/o:microsoft:windows_vista

Following application CPE's matched on the remote system :

  cpe:/a:openssl:openssl:0.9.8r -> OpenSSL Project OpenSSL 0.9.8r
  cpe:/a:modssl:mod_ssl:2.2.21
  cpe:/a:apache:http_server:2.2.21 -> Apache HTTP Server 2.2.21
  cpe:/a:php:php:5.2.17 -> PHP 5.2.17
```

46180 (1) - Additional DNS Hostnames

Synopsis

Potential virtual hosts have been detected.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Different web servers may be hosted on name- based virtual hosts.

See Also

http://en.wikipedia.org/wiki/Virtual_hosting

Solution

If you want to test them, re-scan using the special vhost syntax, such as :
www.example.com[192.0.32.10]

Risk Factor

None

Plugin Information:

Publication date: 2010/04/29, Modification date: 2013/01/21

Hosts

amibaltoledo.es (tcp/0)

```
The following hostnames point to the remote host:
  - www.amibaltoledo.es
```

49704 (1) - External URLs

Synopsis

Links to external sites were gathered.

Description

Nessus gathered HREF links to external sites by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/10/04, Modification date: 2011/08/19

Hosts

amibaltoledo.es (tcp/80)

```
25 external URLs were gathered on this web server :
URL...                                  - Seen on...

http://11/02/2013                       - /listado-de-patocinadores

http://AMIAB                            - /listado-de-patocinadores
http://Ergonalia                        - /listado-de-patocinadores
http://Lozoya                           - /listado-de-patocinadores
http://Previcaman                       - /listado-de-patocinadores
http://aqs                              - /listado-de-patocinadores
http://fitness                          - /listado-de-patocinadores
http://openid.net/                      - /
http://portal.lacaixa.es/home/particulares_es.html - /listado-de-patocinadores
http://www.alquiler-autocares.es/       - /listado-de-patocinadores
http://www.alvarezmartin.com/           - /listado-de-patocinadores
http://www.amibaltoledo.es              - /inauguracion-pagina-web
http://www.ayto-toledo.org              - /listado-de-patocinadores
http://www.clm24.es/articulo/deportes/el-gobierno-municipal-muestra-su-apoyo-al-balonmano-
toledano/20130217114612002951.html - /el-gobierno-municipal-muestra-su-apoyo-al-balonmano-toledano
http://www.diputoledo.es/               - /listado-de-patocinadores
http://www.fbmclm.com/competiciones.asp?v=18&torneo=175 - /
http://www.fbmclm.com/competiciones.asp?v=18&torneo=184 - /
http://www.fbmclm.com/competiciones.asp?v=18&torneo=185 - /
http://www.latribunadetoledo.es/        - /amibal-se-reinventa-para-garantizar-el-futuro
http://www.latribunadetoledo.es/noticia/Z201446B1-9618-95C5-EEDE75A4D68EB1BD/20130203/alvaro/
guimare/anota/in/extremis/amibal/regresa/victoria - /etiquetas/resultados
http://www.latribunadetoledo.es/noticia/ZEDC49721-E4C8-8DB7-1D9C4331BB3E2DA1/20130217/tarde/
tranquila - /
http://www.ortopediatoledo.com/         - /listado-de-patocinadores
http://www.pentatel.es/                 - /listado-de-patocinadores
http://www.rfebm.net/competiciones.asp?v=18&torneo=2899 - /
http://www.youtube.com/embed/DVzdLnUd0-c?wmode=opaque - /no-perdamos-nuestr [...]
```

49705 (1) - Gathered e-mail Addresses

Synopsis

e-mail addresses were gathered.

Description

Nessus gathered mailto: HREF links and extracted e-mail addresses by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/10/04, Modification date: 2011/03/18

Hosts

amibaltoledo.es (tcp/80)

```
The following email address has been gathered :


- 'cdamibaltoledo@gmail.com', referenced from :
   /c%C3%B3mo-apuntarse-al-club-sin-moverse-casa
   /node/63
   /node/64
   /listado-de-patocinadores
   /inscripcion
```

54615 (1) - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/05/23, Modification date: 2011/05/23

Hosts

amibaltoledo.es (tcp/0)

```
Remote device type : general-purpose
Confidence level : 65
```

57323 (1) - OpenSSL Version Detection

Synopsis

The version of OpenSSL can be identified.

Description

The version of OpenSSL could be extracted from the web server's banner. Note that in many cases, security patches are backported and the displayed version number does not show the patch level. Using it to identify vulnerable software is likely to lead to false detections.

See Also

http://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2011/12/16, Modification date: 2011/12/16

Hosts

amibaltoledo.es (tcp/80)

```
Source                : Server: Apache/2.2.21 (Unix) mod_ssl/2.2.21 OpenSSL/0.9.8r
Version (from banner) : 0.9.8r
```