REDdy
Solutions

Nessus Report

Nessus Scan Report
Wed, 01 Nov 2017 19:21:06 EDT

Annex to the Vulnerability Assessment Report
Sample Company

Table Of Contents

Vulnerabilities By Host

192.168.30.157

Scan Information

Start time:	Wed Nov 1 19:11:42 2017
End time:	Wed Nov 1 19:21:06 2017

Host Information

Netbios Name:	Sample Company
IP:	192.168.30.157
MAC Address:	00:0c:29:8b:4d:1a
OS:	Linux Kernel 3.13 on Ubuntu 14.04 (trusty)

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	6	3	60	70

Results Details

0/icmp

10114 - 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 that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Timestamps returned from machines running Windows Vista / 7 / 2008 / 2008 R2 are deliberately incorrect, but usually within 1000 seconds of the actual system time.

Solution

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

Risk Factor

None

References

CVE	CVE-1999-0524
XREF	OSVDB:94
XREF	CWE:200

Plugin Information:

Publication date: 1999/08/01, Modification date: 2012/06/18

Ports

icmp/0

```
The difference between the local and remote clocks is 1 second.
```

0/tcp

11936 - OS Identification

Synopsis

It is possible to guess the remote operating system.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2003/12/09, Modification date: 2017/08/29

Ports

tcp/0

```
Remote operating system : Linux Kernel 3.13 on Ubuntu 14.04 (trusty)
Confidence level : 95
Method : HTTP


The remote host is running Linux Kernel 3.13 on Ubuntu 14.04 (trusty)
```

18261 - 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

Nessus was able to extract the banner of the Apache web server and determine which Linux distribution the remote host is running.

Solution

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

Risk Factor

None

Plugin Information:

Publication date: 2005/05/15, Modification date: 2017/03/13

Ports

tcp/0

```
The Linux distribution detected was :
 - Ubuntu 14.04 (trusty)
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :
- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- 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: 2017/10/26

Ports

tcp/0

```
Information about this scan :

Nessus version : 6.11.2
Plugin feed version : 201711011615
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 192.168.30.156
Port scanner(s) : nessus_syn_scanner
Port range : default
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 : enabled
Web app tests -  Test mode : single
Web app tests -  Try all HTTP methods : no
Web app tests -  Maximum run time : 5 minutes.
Web app tests -  Stop at first flaw : CGI
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2017/11/1 19:11 EDT
Scan duration : 560 sec
```

20094 - VMware Virtual Machine Detection

Synopsis

The remote host is a VMware virtual machine.

Description

According to the MAC address of its network adapter, the remote host is a VMware virtual machine.

Solution

Since it is physically accessible through the network, ensure that its configuration matches your organization's security policy.

Risk Factor

None

Plugin Information:

Publication date: 2005/10/27, Modification date: 2015/10/16

Ports

tcp/0

```
The remote host is a VMware virtual machine.
```

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

35716 - Ethernet Card Manufacturer Detection

Synopsis

The manufacturer can be identified from the Ethernet OUI.

Description

Each ethernet MAC address starts with a 24-bit Organizationally Unique Identifier (OUI). These OUIs are registered by IEEE.

See Also

http://standards.ieee.org/faqs/regauth.html

http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/02/19, Modification date: 2015/10/16

Ports

tcp/0

```
The following card manufacturers were identified :

00:0c:29:8b:4d:1a : VMware, Inc.
```

45590 - Common Platform Enumeration (CPE)

Synopsis

It was 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/

https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/04/21, Modification date: 2017/06/06

Ports

tcp/0

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

  cpe:/o:canonical:ubuntu_linux:14.04

Following application CPE's matched on the remote system :

  cpe:/a:openbsd:openssh:6.6 -> OpenBSD OpenSSH 6.6
  cpe:/a:samba:samba:4.3.11
  cpe:/a:apache:http_server:2.4.7 -> Apache Software Foundation Apache HTTP Server 2.4.7
```

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 : 95
```

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: 2017/08/22

Ports

udp/0

```
For your information, here is the traceroute from 192.168.30.156 to 192.168.30.157 :
192.168.30.156
192.168.30.157

Hop Count: 1
```

22/tcp

90317 - SSH Weak Algorithms Supported

Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

See Also

https://tools.ietf.org/html/rfc4253#section-6.3

Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N)

Plugin Information:

Publication date: 2016/04/04, Modification date: 2016/12/14

Ports

tcp/22

```
The following weak server-to-client encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256

The following weak client-to-server encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256
```

70658 - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining.

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.
Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor

Low

CVSS Base Score

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

CVSS Temporal Score

2.6 (CVSS2#E:ND/RL:ND/RC:ND)

References

BID	32319
CVE	CVE-2008-5161
XREF	OSVDB:50035
XREF	OSVDB:50036
XREF	CERT:958563
XREF	CWE:200

Plugin Information:

Publication date: 2013/10/28, Modification date: 2016/05/12

Ports

tcp/22

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
```

71049 - SSH Weak MAC Algorithms Enabled

Synopsis

The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms.

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.
Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Risk Factor

Low

CVSS Base Score

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

Plugin Information:

Publication date: 2013/11/22, Modification date: 2016/12/14

Ports

tcp/22

```
The following client-to-server Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-sha1-96
  hmac-sha1-96-etm@openssh.com

The following server-to-client Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-sha1-96
```

```
    hmac-sha1-96-etm@openssh.com
```

10267 - 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.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2017/05/30

Ports

tcp/22

```
SSH version : SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.8
SSH supported authentication : publickey,password
```

10881 - 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.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/03/06, Modification date: 2017/05/30

Ports

tcp/22

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

  - 1.99
  - 2.0
```

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 scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/05/22

Ports

tcp/22

```
Port 22/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able 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: 2017/07/07

Ports

tcp/22

```
An SSH server is running on this port.
```

39520 - Backported Security Patch Detection (SSH)

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' 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.

See Also

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/06/25, Modification date: 2015/07/07

Ports

tcp/22

```

Give Nessus credentials to perform local checks.
```

70657 - SSH Algorithms and Languages Supported

Synopsis

An SSH server is listening on this port.

Description

This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2013/10/28, Modification date: 2017/08/28

Ports

tcp/22

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

  curve25519-sha256@libssh.org
  diffie-hellman-group-exchange-sha1
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group1-sha1
  diffie-hellman-group14-sha1
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521

The server supports the following options for server_host_key_algorithms :

  ecdsa-sha2-nistp256
  ssh-dss
  ssh-ed25519
  ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes128-gcm@openssh.com
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  aes256-gcm@openssh.com
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  chacha20-poly1305@openssh.com
  rijndael-cbc@lysator.liu.se

The server supports the following options for encryption_algorithms_server_to_client :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes128-gcm@openssh.com
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  aes256-gcm@openssh.com
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  chacha20-poly1305@openssh.com
  rijndael-cbc@lysator.liu.se

The server supports the following options for mac_algorithms_client_to_server :

  hmac-md5
  hmac-md5-96
  hmac-md5-96-etm@openssh.com
  hmac-md5-etm@openssh.com
  hmac-ripemd160
  hmac-ripemd160-etm@openssh.com
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
```

```
    hmac-sha1-96-etm@openssh.com
    hmac-sha1-etm@openssh.com
    hmac-sha2-256
    hmac-sha2-256-etm@openssh.com
    hmac-sha2-512
    hmac-sha2-512-etm@openssh.com
    umac-128-etm@openssh.com
    umac-128@openssh.com
    umac-64-etm@openssh.com
    umac-64@openssh.com

  The server supports the following options for mac_algorithms_server_to_client :

    hmac-md5
    hmac-md5-96
    hmac-md5-96-etm@openssh.com
    hmac-md5-etm@openssh.com
    hmac-ripemd160
    hmac-ripemd160-etm@openssh.com
    hmac-ripemd160@openssh.com
    hmac-sha1
    hmac-sha1-96
    hmac-sha1-96-etm@openssh.com
    hmac-sh [...]
```

80/tcp

11229 - Web Server info.php / phpinfo.php Detection

Synopsis

The remote web server contains a PHP script that is prone to an information disclosure attack.

Description

Many PHP installation tutorials instruct the user to create a PHP file that calls the PHP function 'phpinfo()' for debugging purposes. Various PHP applications may also include such a file. By accessing such a file, a remote attacker can discover a large amount of information about the remote web server, including :

- The username of the user who installed PHP and if they are a SUDO user.
- The IP address of the host.
- The version of the operating system.
- The web server version.
- The root directory of the web server.
- Configuration information about the remote PHP installation.

Solution

Remove the affected file(s).

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Publication date: 2003/02/12, Modification date: 2013/10/23

Ports

tcp/80

```
  Nessus discovered the following URL that calls phpinfo() :

    - http://192.168.30.157/info.php
```

40984 - Browsable Web Directories

Synopsis

Some directories on the remote web server are browsable.

Description

Multiple Nessus plugins identified directories on the web server that are browsable.

See Also

http://www.nessus.org/u?0a35179e

Solution

Make sure that browsable directories do not leak confidential informative or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

CVSS Base Score

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

Plugin Information:

Publication date: 2009/09/15, Modification date: 2016/12/30

Ports

tcp/80

```
The following directories are browsable :

http://192.168.30.157/Backnode_files/
http://192.168.30.157/apache/
http://192.168.30.157/old/
http://192.168.30.157/test/
http://192.168.30.157/wordpress/wp-content/themes/twentyfifteen/genericons/
http://192.168.30.157/wordpress/wp-includes/
http://192.168.30.157/wordpress/wp-includes/ID3/
http://192.168.30.157/wordpress/wp-includes/IXR/
http://192.168.30.157/wordpress/wp-includes/Requests/
http://192.168.30.157/wordpress/wp-includes/Requests/Auth/
http://192.168.30.157/wordpress/wp-includes/Requests/Cookie/
http://192.168.30.157/wordpress/wp-includes/Requests/Exception/
http://192.168.30.157/wordpress/wp-includes/Requests/Exception/HTTP/
http://192.168.30.157/wordpress/wp-includes/Requests/Exception/Transport/
http://192.168.30.157/wordpress/wp-includes/Requests/Proxy/
http://192.168.30.157/wordpress/wp-includes/Requests/Response/
http://192.168.30.157/wordpress/wp-includes/Requests/Transport/
http://192.168.30.157/wordpress/wp-includes/Requests/Utility/
http://192.168.30.157/wordpress/wp-includes/SimplePie/
http://192.168.30.157/wordpress/wp-includes/SimplePie/Cache/
http://192.168.30.157/wordpress/wp-includes/SimplePie/Content/
http://192.168.30.157/wordpress/wp-includes/SimplePie/Content/Type/
http://192.168.30.157/wordpress/wp-includes/SimplePie/Decode/
http://192.168.30.157/wordpress/wp-includes/SimplePie/Decode/HTML/
http://192.168.30.157/wordpress/wp-includes/SimplePie/HTTP/
http://192.168.30.157/wordpress/wp-includes/SimplePie/Net/
http://192.168.30.157/wordpress/wp-includes/SimplePie/Parse/
http://192.168.30.157/wordpress/wp-includes/SimplePie/XML/
http://192.168.30.157/wordpress/wp-includes/SimplePie/XML/Declaration/
http://192.168.30.157/wordpress/wp-includes/Text/
http://192.168.30.157/wordpress/wp-includes/Text/Diff/
http://192.168.30.157/wordpress/wp-includes/Text/Diff/Engine/
http://192.168.30.157/wordpress/wp-includes/Text/Diff/Renderer/
http://192.168.30.157/wordpress/wp-includes/certificates/
http://192.168.30.157/wordpress/wp-includes/css/
http://19 [...]
```

85582 - Web Application Potentially Vulnerable to Clickjacking

Synopsis

The remote web server may fail to mitigate a class of web application vulnerabilities.

Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions. X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.
Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

See Also

http://www.nessus.org/u?399b1f56

https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet

https://en.wikipedia.org/wiki/Clickjacking

Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.
This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

Risk Factor

Medium

CVSS Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

References

XREF	CWE:693

Plugin Information:

Publication date: 2015/08/22, Modification date: 2017/05/16

Ports

tcp/80

```
The following pages do not use a clickjacking mitigation response header and contain a clickable
 event :

  - http://192.168.30.157/wordpress/
```

90067 - WordPress User Enumeration

Synopsis

The remote web server contains a PHP application that is affected by an information disclosure vulnerability.

Description

The version of WordPress hosted on the remote web server is affected by a user enumeration vulnerability. An unauthenticated, remote attacker can exploit this to learn the names of valid WordPress users.
This information could be used to mount further attacks.

See Also

https://hackertarget.com/wordpress-user-enumeration/

Solution

n/a

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Publication date: 2016/03/21, Modification date: 2016/03/21

Ports

tcp/80

```
Nessus was able to enumerate the following WordPress users from the WordPress install at
 'http://192.168.30.157/wordpress' :
 admin
```

26194 - Web Server Transmits Cleartext Credentials

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
XREF	CWE:928
XREF	CWE:930

Plugin Information:

Publication date: 2007/09/28, Modification date: 2016/11/29

Ports

tcp/80

```
Page : /phpmyadmin/
Destination Page: /phpmyadmin/index.php

Page : /phpmyadmin/index.php
Destination Page: /phpmyadmin/index.php
```

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: 2016/02/19

Ports

tcp/80

```
The remote web server type is :

Apache/2.4.7 (Ubuntu)

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

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 website 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: 2014/05/09

Ports

tcp/80

```
Contents of robots.txt :

User-agent: *
Disallow: /old/
Disallow: /test/
Disallow: /TR2/
Disallow: /Backnode_files/
```

10662 - Web mirroring

Synopsis

Nessus can crawl the remote website.

Description

This plugin makes a mirror of the remote website(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: 2017/10/17

Ports

tcp/80

```
Webmirror performed 1000 queries in 62s (16.0129 queries per second)
```

```
The following CGIs have been discovered :


+ CGI : /wordpress/
  Methods : GET
  Argument : feed
   Value: comments-rss2
  Argument : p
   Value: 1#comments
  Argument : s


+ CGI : /wordpress/index.php
  Methods : GET
  Argument : rest_route
   Value: /


+ CGI : /wordpress/xmlrpc.php
  Methods : GET
  Argument :
   Value: rsd


+ CGI : /phpmyadmin/phpmyadmin.css.php
  Methods : GET
  Argument : collation_connection
   Value: utf8_general_ci
  Argument : lang
   Value: en
  Argument : nocache
   Value: 4147360344ltr
  Argument : server
   Value: 1
  Argument : token
   Value: 5db87be3c0bffdcb2d97b56db50ea868


+ CGI : /phpmyadmin/url.php
  Methods : GET
  Argument : collation_connection
   Value: utf8_general_ci
  Argument : lang
   Value: en
  Argument : token
   Value: 5db87be3c0bffdcb2d97b56db50ea868
  Argument : url
   Value: http%3A%2F%2Fdocs.phpmyadmin.net%2Fen%2Flatest%2Findex.html


+ CGI : /phpmyadmin/index.php
  Methods : GET,POST
  Argument : collation_connection
   Value: utf8_general_ci
  Argument : db
  Argument : lang
   Value: zh_TW
  Argument : pma_password
  Argument : pma_username
  Argument : server
   Value: 1
  Argument : table
  Argument : target
   Value: index.php
  Argument : token
   Value: 5db87be3c0bffdcb2d97b56db50ea868


+ CGI : /wordpress/wp-includes/js/
  Methods : GET
  Argument : item

Directory index found at /Backnode_files/
Directory index found at /test/
Directory index found at /old/
Directory index found at /apache/
Directory index found at /wordpress/wp-content/themes/twentyfifteen/genericons/
Directory index found at /wordpress/wp-includes/
Directory index found at /wordpress/wp-includes/ID3/
Directory index found at /wordpress/wp-includes/IXR/
Directory index found at /wordpress/wp-includes/Requests/
Directory index found at /wordpress/wp-includes/SimplePie/
Directory index found at /wordpress/wp-includes/Text/
Directory index found at /wordpress/wp-includes/certificates/
Directory index found at / [...]
```

11032 - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

http://projects.webappsec.org/Predictable-Resource-Location

Solution

n/a

Risk Factor

None

References

XREF	OWASP:OWASP-CM-006

Plugin Information:

Publication date: 2002/06/26, Modification date: 2015/10/13

Ports

tcp/80

```
The following directories were discovered:
/old, /test, /apache, /icons, /javascript, /phpmyadmin, /wordpress, //old, //test, //
Backnode_files

While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

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 scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/05/22

Ports

tcp/80

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

17219 - phpMyAdmin Detection

Synopsis

The remote web server hosts a database management application written in PHP.

Description

The remote host is running phpMyAdmin, a web-based MySQL administration tool written in PHP.

See Also

https://www.phpmyadmin.net/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/02/25, Modification date: 2016/04/12

Ports

tcp/80

```

The following instance of phpMyAdmin was detected on the remote host :

  Version : unknown
  URL     : http://192.168.30.157/phpmyadmin/
```

18297 - WordPress Detection

Synopsis

The remote web server contains a blog application written in PHP.

Description

The remote host is running WordPress, a free blog application written in PHP with a MySQL back-end.

See Also

http://www.wordpress.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/05/18, Modification date: 2016/12/09

Ports

tcp/80

```

  URL     : http://192.168.30.157/wordpress
  Version : 4.8.3
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able 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: 2017/07/07

Ports

tcp/80

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

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: Wed, 01 Nov 2017 23:14:48 GMT
  Server: Apache/2.4.7 (Ubuntu)
  Last-Modified: Sun, 06 Aug 2017 05:02:15 GMT
  ETag: "8ce8-5560ea23d23c0"
  Accept-Ranges: bytes
  Content-Length: 36072
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html
```

33817 - CGI Generic Tests Load Estimation (all tests)

Synopsis

Load estimation for web application tests.

Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.
The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.
Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/10/26, Modification date: 2014/03/12

Ports

tcp/80

```
Here are the estimated number of requests in miscellaneous modes
```

```
for one method only (GET or POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

on site request forgery                  : S=3          SP=3         AP=3         SC=3
 AC=3
SQL injection                            : S=552        SP=1368      AP=1368      SC=3072
 AC=3072
unseen parameters                        : S=805        SP=1995      AP=1995      SC=4480
 AC=4480
local file inclusion                     : S=23         SP=57        AP=57        SC=128
 AC=128
web code injection                       : S=23         SP=57        AP=57        SC=128
 AC=128
XML injection                            : S=23         SP=57        AP=57        SC=128
 AC=128
format string                            : S=46         SP=114       AP=114       SC=256
 AC=256
script injection                         : S=3          SP=3         AP=3         SC=3
 AC=3
cross-site scripting (comprehensive test): S=92         SP=228       AP=228       SC=512
 AC=512
injectable parameter                     : S=46         SP=114       AP=114       SC=256
 AC=256
cross-site scripting (extended patterns) : S=18         SP=18        AP=18        SC=18
 AC=18
directory traversal (write access)       : S=46         SP=114       AP=114       SC=256
 AC=256
SSI injection                            : S=69         SP=171       AP=171       SC=384
 AC=384
header injection                         : S=6          SP=6         AP=6         SC=6
 AC=6
directory traversal                      : S=575        SP=1425      AP=1425      SC=3200
 AC=3200
HTML injection                           : S=15         SP=15        AP=15        SC=15
 AC=15
arbitrary command execution (time based) : S=138        SP=342       AP=342       SC=768
 AC=768
persistent XSS                         [...]
```

39470 - CGI Generic Tests Timeout

Synopsis

Some generic CGI attacks ran out of time.

Description

Some generic CGI tests ran out of time during the scan. The results may be incomplete.

Solution

Consider increasing the 'maximum run time (minutes)' preference for the 'Web Applications Settings' in order to prevent the CGI scanning from timing out. Less ambitious options could also be used, such as :
- Test more that one parameter at a time per form :
'Test all combinations of parameters' is much slower than 'Test random pairs of parameters' or 'Test all pairs of parameters (slow)'.
- 'Stop after one flaw is found per web server (fastest)'
under 'Do not stop after the first flaw is found per web page' is quicker than 'Look for all flaws (slowest)'.
- In the Settings/Advanced menu, try reducing the value for 'Max number of concurrent TCP sessions per host' or 'Max simultaneous checks per host'.

Risk Factor

None

Plugin Information:

Publication date: 2009/06/19, Modification date: 2016/09/21

Ports

tcp/80

```
The following tests timed out without finding any flaw :
- SQL injection (on HTTP headers)
- SQL injection
```

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

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/06/25, Modification date: 2015/07/07

Ports

tcp/80

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

42057 - Web Server Allows Password Auto-Completion

Synopsis

The 'autocomplete' attribute is not disabled on password fields.

Description

The remote web server contains at least one HTML form field that has 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 if 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: 2016/06/16

Ports

tcp/80

```
Page : /phpmyadmin/
Destination Page: /phpmyadmin/index.php

Page : /phpmyadmin/index.php
Destination Page: /phpmyadmin/index.php
```

43111 - HTTP Methods Allowed (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.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2009/12/10, Modification date: 2013/05/09

Ports

tcp/80

```
Based on the response to an OPTIONS request :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    //Backnode_files
    //old
    //test
    /Backnode_files
    /apache
    /icons
    /javascript
    /old
    /phpmyadmin/themes
    /phpmyadmin/themes/pmahomme
    /phpmyadmin/themes/pmahomme/jquery
    /test
    /wordpress/wp-content/themes/twentyfifteen/genericons
    /wordpress/wp-includes


Based on tests of each method :

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
    //Backnode_files
    //old
    //test
    /Backnode_files
    /apache
    /icons
    /javascript
    /old
    /phpmyadmin
    /phpmyadmin/themes
    /phpmyadmin/themes/pmahomme
    /phpmyadmin/themes/pmahomme/jquery
    /test
    /wordpress
    /wordpress/wp-content
    /wordpress/wp-content/themes
    /wordpress/wp-content/themes/twentyfifteen
    /wordpress/wp-content/themes/twentyfifteen/genericons
    /wordpress/wp-includes
```

47830 - CGI Generic Injectable Parameter

Synopsis

Some CGIs are candidate for extended injection tests.

Description

Nessus was able to to inject innocuous strings into CGI parameters and read them back in the HTTP response.
The affected parameters are candidates for extended injection tests like cross-site scripting attacks.
This is not a weakness per se, the main purpose of this test is to speed up other scripts. The results may be useful for a human pen-tester.

Solution

n/a

Risk Factor

None

References

XREF	CWE:86

Plugin Information:

Publication date: 2010/07/26, Modification date: 2017/01/05

Ports

tcp/80

```
Using the GET HTTP method, Nessus found that :

+ The following resources may be vulnerable to injectable parameter :

+ The 's' parameter of the /wordpress/ CGI :

/wordpress/?s=fxnbai

-------- output --------
<![endif]-->
<script>(function(html){html.className = html.className.replace(/\ [...]
<title>Search Results for &#8220;fxnbai&#8221; &#8211; Web_TR2</title>
<meta name='robots' content='noindex,follow' />
<link rel='dns-prefetch' href='//fonts.googleapis.com' />
------------------------

+ The 'lang' parameter of the /phpmyadmin/url.php CGI :

/phpmyadmin/url.php?lang=fxnbai

-------- output --------
<fieldset class="tblFooters">
<input value="Go" type="submit" id="input_go" /><input type="hidde [...]
</form><div><div class="error"><img src="themes/dot.gif" title="" alt=""
 class="icon ic_s_error" /> Unknown language: fxnbai.</div></div></div><
/div></body></html>
------------------------

+ The 'target' parameter of the /phpmyadmin/index.php CGI :

/phpmyadmin/index.php?target=fxnbai

-------- output --------
</div>    <input type="hidden" name="server" value="1" /></fieldset>
<fieldset class="tblFooters">
<input value="Go" type="submit" id="input_go" /><input type="hidden" nam
e="target" value="fxnbai" /><input type="hidden" name="lang" value="en"
/><input type="hidden" name="collation_connection" value="utf8_general_c
i" /><input type="hidden" name="token" value="16980402ab035ea0327fd06b30
1f2ade" /></fieldset>
</form></div></div></body></html>
------------------------

Clicking directly on these URLs should exhibit the issue :
(you will probably need to read the HTML source)

http://192.168.30.157/wordpress/?s=fxnbai
http://192.168.30.157/phpmyadmin/url.php?lang=fxnbai
http://192.168.30.157/phpmyadmin/index.php?target=fxnbai
```

48243 - PHP Version Detection

Synopsis

It was possible to obtain the version number of the remote PHP installation.

Description

Nessus was able to determine the version of PHP available on the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/08/04, Modification date: 2017/07/07

Ports

tcp/80

```
Nessus was able to identify the following PHP version information :

  Version : 5.5.9-1ubuntu4.22
  Source  : X-Powered-By: PHP/5.5.9-1ubuntu4.22
  Source  : http://192.168.30.157/info.php
```

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

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


http://fonts.googleapis.com             - /wordpress/
http://gmpg.org/xfn/11                  - /wordpress/
http://s.w.org                          - /wordpress/
https://fonts.googleapis.com/css?family=Noto+Sans%3A400italic%2C700italic%2C400%2C700%7CNoto
+Serif%3A400italic%2C700italic%2C400%2C700%7CInconsolata%3A400%2C700&subset=latin%2Clatin-ext - /
wordpress/
https://fonts.gstatic.com               - /wordpress/
https://github.com/silexlabs/silex-templates/ - /
https://pages.github.com/               - /
https://twitter.com/wordpress           - /wordpress/
https://wordpress.org/                  - /wordpress/
https://www.facebook.com/wordpress      - /wordpress/
https://www.instagram.com/explore/tags/wordcamp/ - /wordpress/
https://www.silex.me/                   - /
https://www.yelp.com                    - /wordpress/
```

49705 - Web Server Harvested Email Addresses

Synopsis

Email addresses were harvested from the web server.

Description

Nessus harvested HREF mailto: links and extracted email addresses by crawling the remote web server.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2010/10/04, Modification date: 2014/01/17

Ports

tcp/80

```
The following email address has been gathered :


- 'wordpress@example.com', referenced from :
   /wordpress/
```

50344 - Missing or Permissive Content-Security-Policy HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) response header or does not set one at all.
The CSP header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

http://content-security-policy.com/

https://www.w3.org/TR/CSP2/

Solution

Set a properly configured Content-Security-Policy header for all requested resources.

Risk Factor

None

Plugin Information:

Publication date: 2010/10/26, Modification date: 2016/04/14

Ports

tcp/80

```
The following pages do not set a Content-Security-Policy response header or set a permissive
 policy:

  - http://192.168.30.157/
  - http://192.168.30.157/Backnode_files/
  - http://192.168.30.157/apache/
  - http://192.168.30.157/old/
  - http://192.168.30.157/phpmyadmin/
  - http://192.168.30.157/phpmyadmin/index.php
  - http://192.168.30.157/test/
  - http://192.168.30.157/wordpress/
  - http://192.168.30.157/wordpress/wp-content/
  - http://192.168.30.157/wordpress/wp-content/themes/
  - http://192.168.30.157/wordpress/wp-content/themes/twentyfifteen/genericons/
  - http://192.168.30.157/wordpress/wp-includes/
  - http://192.168.30.157/wordpress/wp-includes/ID3/
  - http://192.168.30.157/wordpress/wp-includes/ID3/getid3.lib.php
  - http://192.168.30.157/wordpress/wp-includes/ID3/getid3.php
  - http://192.168.30.157/wordpress/wp-includes/IXR/
  - http://192.168.30.157/wordpress/wp-includes/IXR/class-IXR-base64.php
  - http://192.168.30.157/wordpress/wp-includes/IXR/class-IXR-client.php
  - http://192.168.30.157/wordpress/wp-includes/IXR/class-IXR-date.php
  - http://192.168.30.157/wordpress/wp-includes/IXR/class-IXR-error.php
  - http://192.168.30.157/wordpress/wp-includes/IXR/class-IXR-message.php
  - http://192.168.30.157/wordpress/wp-includes/IXR/class-IXR-request.php
  - http://192.168.30.157/wordpress/wp-includes/IXR/class-IXR-server.php
  - http://192.168.30.157/wordpress/wp-includes/IXR/class-IXR-value.php
  - http://192.168.30.157/wordpress/wp-includes/Requests/
  - http://192.168.30.157/wordpress/wp-includes/Requests/Auth.php
  - http://192.168.30.157/wordpress/wp-includes/Requests/Auth/
  - http://192.168.30.157/wordpress/wp-includes/Requests/Cookie.php
  - http://192.168.30.157/wordpress/wp-includes/Requests/Cookie/
  - http://192.168.30.157/wordpress/wp-includes/Requests/Cookie/Jar.php
  - http://192.168.30.157/wordpress/wp-includes/Requests/Exception.php
  - http://192.168.30.157/wordpress/wp-includes/Requests/Exception/
  - http://192.168.30.157/wordpress/wp-includes/Requests/Exception/HTTP/
  -  [...]
```

50345 - Missing or Permissive X-Frame-Options HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all.
The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

See Also

https://en.wikipedia.org/wiki/Clickjacking

http://www.nessus.org/u?399b1f56

Solution

Set a properly configured X-Frame-Options header for all requested resources.

Risk Factor

None

Plugin Information:

Publication date: 2010/10/26, Modification date: 2017/05/16

Ports

tcp/80

```
The following pages do not set a X-Frame-Options response header or set a permissive policy:

  - http://192.168.30.157/
  - http://192.168.30.157/Backnode_files/
  - http://192.168.30.157/apache/
  - http://192.168.30.157/old/
  - http://192.168.30.157/test/
  - http://192.168.30.157/wordpress/
  - http://192.168.30.157/wordpress/wp-content/
  - http://192.168.30.157/wordpress/wp-content/themes/
  - http://192.168.30.157/wordpress/wp-content/themes/twentyfifteen/genericons/
  - http://192.168.30.157/wordpress/wp-includes/
  - http://192.168.30.157/wordpress/wp-includes/ID3/
  - http://192.168.30.157/wordpress/wp-includes/ID3/getid3.lib.php
  - http://192.168.30.157/wordpress/wp-includes/ID3/getid3.php
  - http://192.168.30.157/wordpress/wp-includes/IXR/
  - http://192.168.30.157/wordpress/wp-includes/IXR/class-IXR-base64.php
  - http://192.168.30.157/wordpress/wp-includes/IXR/class-IXR-client.php
  - http://192.168.30.157/wordpress/wp-includes/IXR/class-IXR-date.php
  - http://192.168.30.157/wordpress/wp-includes/IXR/class-IXR-error.php
  - http://192.168.30.157/wordpress/wp-includes/IXR/class-IXR-message.php
  - http://192.168.30.157/wordpress/wp-includes/IXR/class-IXR-request.php
  - http://192.168.30.157/wordpress/wp-includes/IXR/class-IXR-server.php
  - http://192.168.30.157/wordpress/wp-includes/IXR/class-IXR-value.php
  - http://192.168.30.157/wordpress/wp-includes/Requests/
  - http://192.168.30.157/wordpress/wp-includes/Requests/Auth.php
  - http://192.168.30.157/wordpress/wp-includes/Requests/Auth/
  - http://192.168.30.157/wordpress/wp-includes/Requests/Cookie.php
  - http://192.168.30.157/wordpress/wp-includes/Requests/Cookie/
  - http://192.168.30.157/wordpress/wp-includes/Requests/Cookie/Jar.php
  - http://192.168.30.157/wordpress/wp-includes/Requests/Exception.php
  - http://192.168.30.157/wordpress/wp-includes/Requests/Exception/
  - http://192.168.30.157/wordpress/wp-includes/Requests/Exception/HTTP/
  - http://192.168.30.157/wordpress/wp-includes/Requests/Exception/Transport/
  - http://192.168. [...]
```

84574 - Backported Security Patch Detection (PHP)

Synopsis

Security patches have been backported.

Description

Security patches may have been 'backported' to the remote PHP install 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

https://access.redhat.com/security/updates/backporting/?sc_cid=3093

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2015/07/07, Modification date: 2015/07/07

Ports

tcp/80

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

85602 - Web Application Cookies Not Marked Secure

Synopsis

HTTP session cookies might be transmitted in cleartext.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session.
However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies.
Note that this plugin detects all general cookies missing the 'secure'
cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag.

See Also

https://www.owasp.org/index.php/SecureFlag

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.
If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data.

Risk Factor

None

References

XREF	CWE:522
XREF	CWE:718
XREF	CWE:724
XREF	CWE:928
XREF	CWE:930

Plugin Information:

Publication date: 2015/08/24, Modification date: 2015/08/24

Ports

tcp/80

```
The following cookies do not set the secure cookie flag :

Name : pma_lang
Path : /phpmyadmin/
Value : en
Domain :
Version : 1
Expires : Fri, 01-Dec-2017 23:13:17 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : pma_collation_connection
Path : /phpmyadmin/
Value : utf8_general_ci
Domain :
Version : 1
Expires : Fri, 01-Dec-2017 23:13:17 GMT
Comment :
Secure : 0
Httponly : 1
Port :


Name : phpMyAdmin
Path : /phpmyadmin/
Value : m99dkm788rse4rim3p4304r52rjjddrd
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 1
Port :
```

91815 - Web Application Sitemap

Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

See Also

http://www.nessus.org/u?5496c8d9

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2016/06/24, Modification date: 2016/06/24

Ports

tcp/80

```
The following sitemap was created from crawling linkable content on the target host :

  - http://192.168.30.157/
  - http://192.168.30.157/Backnode_files/
  - http://192.168.30.157/Backnode_files/
AAEAAQAAAAAAAAdJAAAAJDhiNGY1YTk3LTQ3NTctNDE1Ny1hZmU4LTlhMWE4.jpg
  - http://192.168.30.157/Backnode_files/failure-good-thing-fixed.png
  - http://192.168.30.157/Backnode_files/front-end.css
  - http://192.168.30.157/Backnode_files/front-end.js
  - http://192.168.30.157/Backnode_files/jquery-ui.js
  - http://192.168.30.157/Backnode_files/jquery.js
  - http://192.168.30.157/Backnode_files/logo.png
  - http://192.168.30.157/Backnode_files/normalize.css
  - http://192.168.30.157/Backnode_files/pageable.js
  - http://192.168.30.157/Backnode_files/picto1.png
  - http://192.168.30.157/Backnode_files/picto2.png
  - http://192.168.30.157/Backnode_files/picto3.png
  - http://192.168.30.157/Backnode_files/script.json
  - http://192.168.30.157/Backnode_files/styles.css
  - http://192.168.30.157/Backnode_files/tumblr_lb4pi2yt1C1qb2xivo1_500.gif
  - http://192.168.30.157/apache/
  - http://192.168.30.157/old/
  - http://192.168.30.157/phpmyadmin/
  - http://192.168.30.157/phpmyadmin/favicon.ico
  - http://192.168.30.157/phpmyadmin/index.php
  - http://192.168.30.157/phpmyadmin/phpmyadmin.css.php
  - http://192.168.30.157/phpmyadmin/themes/pmahomme/jquery/jquery-ui-1.9.2.custom.css
  - http://192.168.30.157/test/
  - http://192.168.30.157/wordpress/
  - http://192.168.30.157/wordpress/wp-content/
  - http://192.168.30.157/wordpress/wp-content/themes/
  - http://192.168.30.157/wordpress/wp-content/themes/twentyfifteen/genericons/
  - http://192.168.30.157/wordpress/wp-content/themes/twentyfifteen/genericons/COPYING.txt
  - http://192.168.30.157/wordpress/wp-content/themes/twentyfifteen/genericons/Genericons.eot
  - http://192.168.30.157/wordpress/wp-content/themes/twentyfifteen/genericons/Genericons.svg
  - http://192.168.30.157/wordpress/wp-content/themes/twentyfifteen/genericons/Genericons.ttf
  - http://192.168.30.157/wordpress/wp-c [...]
```

101842 - WordPress Plugin Detection

Synopsis

The remote WordPress application has plugins installed

Description

The WordPress application running on the remote host has plugins installed.

See Also

https://wordpress.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2017/07/20, Modification date: 2017/10/17

Ports

tcp/80

```
Plugin : Version
Akismet : 3.3.3

Themes:
twentyseventeen
twentyfifteen
twentysixteen
```

137/udp

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure

Synopsis

It was possible to obtain the network name of the remote host.

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests. Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 1999/10/12, Modification date: 2017/09/27

Ports

udp/137

```
The following 7 NetBIOS names have been gathered :

 LAZYSYSADMIN      = Computer name
 LAZYSYSADMIN      = Messenger Service
 LAZYSYSADMIN      = File Server Service
 __MSBROWSE__      = Master Browser
 WORKGROUP         = Workgroup / Domain name
 WORKGROUP         = Master Browser
 WORKGROUP         = Browser Service Elections

This SMB server seems to be a Samba server - its MAC address is NULL.
```

139/tcp

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/06/05, Modification date: 2015/06/02

Ports

tcp/139

```

An SMB server is running on this port.
```

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 scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/05/22

Ports

tcp/139

```
Port 139/tcp was found to be open
```

445/tcp

42411 - Microsoft Windows SMB Shares Unprivileged Access

Synopsis

It is possible to access a network share.

Description

The remote has one or more Windows shares that can be accessed through the network with the given credentials. Depending on the share rights, it may allow an attacker to read/write confidential data.

Solution

To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing' tab, and click on 'permissions'.

Risk Factor

High

CVSS Base Score

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

CVSS Temporal Score

7.5 (CVSS2#E:H/RL:U/RC:ND)

References

BID	8026
CVE	CVE-1999-0519
CVE	CVE-1999-0520
XREF	OSVDB:299

Plugin Information:

Publication date: 2009/11/06, Modification date: 2011/03/27

Ports

tcp/445

```
The following shares can be accessed using a NULL session  :

- share$  - (readable)
  + Content of this share :
..
wordpress
Backnode_files
wp
deets.txt
robots.txt
todolist.txt
apache
index.html
info.php
test
old
```

57608 - SMB Signing Disabled

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

See Also

https://support.microsoft.com/en-us/kb/887429 http://technet.microsoft.com/en-us/library/cc731957.aspx

http://www.nessus.org/u?74b80723

http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html

http://www.nessus.org/u?a3cac4ea

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Risk Factor

Medium

CVSS Base Score

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

CVSS Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

Plugin Information:

Publication date: 2012/01/19, Modification date: 2016/12/09

Ports

tcp/445

10394 - Microsoft Windows SMB Log In Possible

Synopsis

It was possible to log into the remote host.

Description

The remote host is running a Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts :
- NULL session
- Guest account
- Supplied credentials

See Also

http://support.microsoft.com/kb/143474

http://support.microsoft.com/kb/246261

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2017/01/19

Ports

tcp/445

```
- NULL sessions are enabled on the remote host.
```

10395 - Microsoft Windows SMB Shares Enumeration

Synopsis

It is possible to enumerate remote network shares.

Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2015/01/12

Ports

tcp/445

```

Here are the SMB shares available on the remote host :

  - print$
  - share$
  - IPC$
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

Synopsis

It was possible to obtain information about the remote operating system.

Description

Nessus was able to obtain the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Note that this plugin requires SMB1 to be enabled on the host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2001/10/17, Modification date: 2017/02/21

Ports

tcp/445

```
The remote Operating System is : Windows 6.1
The remote native LAN manager is : Samba 4.3.11-Ubuntu
The remote SMB Domain Name is : LAZYSYSADMIN
```

10859 - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

Synopsis

It is possible to obtain the host SID for the remote host.

Description

By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier).
The host SID can then be used to get the list of local users.

See Also

http://technet.microsoft.com/en-us/library/bb418944.aspx

Solution

You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.
Refer to the 'See also' section for guidance.

Risk Factor

None

References

BID	959
CVE	CVE-2000-1200
XREF	OSVDB:715

Plugin Information:

Publication date: 2002/02/13, Modification date: 2015/11/18

Ports

tcp/445

```
The remote host SID value is :

1-5-21-2952042175-1524911573-1237092750

The value of 'RestrictAnonymous' setting is : unknown
```

10860 - SMB Use Host SID to Enumerate Local Users

Synopsis

Nessus was able to enumerate local users.

Description

Using the host security identifier (SID), Nessus was able to enumerate local users on the remote Windows system.

Solution

n/a

Risk Factor

None

References

XREF	OSVDB:714

Plugin Information:

Publication date: 2002/02/13, Modification date: 2017/02/02

Ports

tcp/445

```
  - nobody (id 501, Guest account)

Note that, in addition to the Administrator and Guest accounts, Nessus
has enumerated only those local users with IDs between 1000 and 1200.
To use a different range, edit the scan policy and change the 'Start
UID' and/or 'End UID' preferences for this plugin, then re-run the
scan.
```

11011 - Microsoft Windows SMB Service Detection

Synopsis

A file / print sharing service is listening on the remote host.

Description

The remote service understands the CIFS (Common Internet File System) or Server Message Block (SMB) protocol, used to provide shared access to files, printers, etc between nodes on a network.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/06/05, Modification date: 2015/06/02

Ports

tcp/445

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

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 scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/05/22

Ports

tcp/445

```
Port 445/tcp was found to be open
```

17651 - Microsoft Windows SMB : Obtains the Password Policy

Synopsis

It is possible to retrieve the remote host's password policy using the supplied credentials.

Description

Using the supplied credentials it was possible to extract the password policy for the remote Windows host. The password policy must conform to the Informational System Policy.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/03/30, Modification date: 2015/01/12

Ports

tcp/445

```
The following password policy is defined on the remote host:

Minimum password len: 5
Password history len: 0
Maximum password age (d): No limit
Password must meet complexity requirements: Disabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 1800
Time between failed logon (s): 1800
Number of invalid logon before locked out (s): 0
```

25240 - Samba Server Detection

Synopsis

An SMB server is running on the remote host.

Description

The remote host is running Samba, a CIFS/SMB server for Linux and Unix.

See Also

http://www.samba.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2013/01/07

Ports

tcp/445

60119 - Microsoft Windows SMB Share Permissions Enumeration

Synopsis

It was possible to enumerate the permissions of remote network shares.

Description

By using the supplied credentials, Nessus was able to enumerate the permissions of network shares. User permissions are enumerated for each network share that has a list of access control entries (ACEs).

See Also

https://technet.microsoft.com/en-us/library/bb456988.aspx

https://technet.microsoft.com/en-us/library/cc783530.aspx

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2012/07/25, Modification date: 2017/02/27

Ports

tcp/445

```
Share path : \\LAZYSYSADMIN\print$
Local path : C:\var\lib\samba\printers
Comment : Printer Drivers
[*] Allow ACE for Everyone: 0x001f01ff
    FILE_ALL_ACCESS:           YES
    FILE_ALL_ACCESS:           YES
    FILE_ALL_ACCESS:           YES

Share path : \\LAZYSYSADMIN\share$
Local path : C:\var\www\html\
Comment : Sumshare
[*] Allow ACE for Everyone: 0x001f01ff
    FILE_ALL_ACCESS:           YES
    FILE_ALL_ACCESS:           YES
    FILE_ALL_ACCESS:           YES

Share path : \\LAZYSYSADMIN\IPC$
Local path : C:\tmp
Comment : IPC Service (Web server)
[*] Allow ACE for Everyone: 0x001f01ff
    FILE_ALL_ACCESS:           YES
    FILE_ALL_ACCESS:           YES
    FILE_ALL_ACCESS:           YES
```

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)

Synopsis

The remote Windows host supports the SMBv1 protocol.

Description

The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues.

See Also

https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/

https://support.microsoft.com/en-us/kb/2696547

http://www.nessus.org/u?8dcab5e4

http://www.nessus.org/u?36fd3072

http://www.nessus.org/u?4c7e0cf3

Solution

Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk Factor

None

References

XREF	OSVDB:151058

Plugin Information:

Publication date: 2017/02/03, Modification date: 2017/02/16

Ports

tcp/445

```
The remote host supports SMBv1.
```

100871 - Microsoft Windows SMB Versions Supported (remote check)

Synopsis

It was possible to obtain information about the version of SMB running on the remote host.

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.
Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2017/06/19, Modification date: 2017/06/19

Ports

tcp/445

```
The remote host supports the following versions of SMB :
  SMBv1
  SMBv2
```

3306/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 scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/05/22

Ports

tcp/3306

```
Port 3306/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able 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: 2017/07/07

Ports

tcp/3306

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

6667/tcp

11156 - IRC Daemon Version Detection

Synopsis

The remote host is an IRC server.

Description

This plugin determines the version of the IRC daemon.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2002/11/19, Modification date: 2016/01/08

Ports

tcp/6667

```
The IRC server version is : :InspIRCd-2.0
```

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 scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2017/05/22

Ports

tcp/6667

```
Port 6667/tcp was found to be open
```

22964 - Service Detection

Synopsis

The remote service could be identified.

Description

Nessus was able 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: 2017/07/07

Ports

tcp/6667

```
An IRC server is running on this port.
```

REDdy
Solutions