BNS_sitiopruebasIP

Report generated by Nessus™

Thu, 14 Nov 2019 19:09:06 CST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

165.22.34.38

0	0	4	1	46
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Thu Nov 14 15:29:10 2019
End time:	Thu Nov 14 19:09:06 2019

Host Information

IP:	165.22.34.38
OS:	AIX 5.3

Vulnerabilities

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

Published: 2009/09/15, Modified: 2016/12/30

Plugin Output

tcp/80

```

The following directories are browsable :

http://165.22.34.38/css/
http://165.22.34.38/css/lightbox/
http://165.22.34.38/images/
http://165.22.34.38/images/design/
http://165.22.34.38/images/fonts/
http://165.22.34.38/images/icon/
http://165.22.34.38/images/portfolio/
http://165.22.34.38/images/portfolio/tooltips/
http://165.22.34.38/images/slider/
http://165.22.34.38/images/thumbs/
http://165.22.34.38/js/
```

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

Published: 2009/09/15, Modified: 2016/12/30

Plugin Output

tcp/443

```
The following directories are browsable :

https://165.22.34.38/css/
https://165.22.34.38/css/lightbox/
https://165.22.34.38/images/
https://165.22.34.38/images/design/
https://165.22.34.38/images/fonts/
https://165.22.34.38/images/icon/
https://165.22.34.38/images/portfolio/
https://165.22.34.38/images/portfolio/tooltips/
https://165.22.34.38/images/slider/
https://165.22.34.38/images/thumbs/
```

```
https://165.22.34.38/js/
```

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

Published: 2015/08/22, Modified: 2017/05/16

Plugin Output

tcp/80

```

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

  - http://165.22.34.38/contact.htm
```

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

Published: 2015/08/22, Modified: 2017/05/16

Plugin Output

tcp/443

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

  - https://165.22.34.38/contact.htm
```

95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)

Synopsis

A known CA SSL certificate in the certificate chain has been signed using a weak hashing algorithm.

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing the attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

See Also

https://tools.ietf.org/html/rfc3279

https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2008/961509

Solution

Contact the Certificate Authority to have the certificate reissued.

Risk Factor

Medium

CVSS Base Score

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

References

BID	11849
BID	33065
CVE	CVE-2004-2761
XREF	CERT:836068
XREF	CWE:310

Plugin Information

Published: 2016/12/08, Modified: 2019/11/13

Plugin Output

tcp/443

```
The following known CA certificates were part of the certificate
chain sent by the remote host, but contain hashes that are considered
to be weak.

|-Subject             : O=Digital Signature Trust Co./CN=DST Root CA X3
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Sep 30 21:12:19 2000 GMT
|-Valid To            : Sep 30 14:01:15 2021 GMT
```

46180 - Additional DNS Hostnames

Synopsis

Nessus has detected potential virtual hosts.

Description

Hostnames different from the current hostname have been collected by miscellaneous plugins. Nessus has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

See Also

https://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

Published: 2010/04/29, Modified: 2017/04/27

Plugin Output

tcp/0

```
The following hostnames point to the remote host :
  - sitiodepruebas.org
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/07/30, Modified: 2019/06/04

Plugin Output

tcp/80

```
URL        : http://165.22.34.38/
Version    : 2.4.99
backported : 1
os         : ConvertedUbuntu
```

48204 - Apache HTTP Server Version

Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/07/30, Modified: 2019/06/04

Plugin Output

tcp/443

```
URL        : https://165.22.34.38/
Version    : 2.4.99
backported : 1
os         : ConvertedUbuntu
```

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

Published: 2010/04/21

Plugin Output

tcp/0

```

The remote operating system matched the following CPE :

  cpe:/o:ibm:aix:5.3 -> IBM AIX 5.3

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server:2.4.29 -> Apache Software Foundation Apache HTTP Server 2.4.29
  cpe:/a:apache:http_server:2.4.99
  cpe:/a:jquery:jquery:2.1.3
```

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

Published: 2011/05/23, Modified: 2011/05/23

Plugin Output

tcp/0

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

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

Published: 2010/10/04, Modified: 2011/08/19

Plugin Output

tcp/80

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


http://fonts.googleapis.com/css?
family=Lato:400,400italic,700,700italic,900,900italic,300italic,300,100italic,100 - /
http://www.freeplantillas.com/          - /
https://chuiso.com/como-hacer-ataques-ddos/ - /
https://sitiodepruebas.org              - /
https://twitter.com/DM20911             - /
https://www.youtube.com/watch?v=XqZsoesa55w - /
```

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

Published: 2010/10/04, Modified: 2011/08/19

Plugin Output

tcp/443

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


http://fonts.googleapis.com/css?
family=Lato:400,400italic,700,700italic,900,900italic,300italic,300,100italic,100 -
http://www.freeplantillas.com/          -
https://chuiso.com/como-hacer-ataques-ddos/ -
https://sitiodepruebas.org              -
https://twitter.com/DM20911             -
https://www.youtube.com/watch?v=XqZsoesa55w -
```

84502 - HSTS Missing From HTTPS Server

Synopsis

The remote web server is not enforcing HSTS.

Description

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

See Also

https://tools.ietf.org/html/rfc6797

Solution

Configure the remote web server to use HSTS.

Risk Factor

None

Plugin Information

Published: 2015/07/02, Modified: 2019/09/20

Plugin Output

tcp/443

```
The remote HTTPS server does not send the HTTP
"Strict-Transport-Security" header.
```

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.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

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.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2019/03/19

Plugin Output

tcp/80

```
Based on the response to an OPTIONS request :
    - HTTP methods GET HEAD OPTIONS POST are allowed on :

      /
      /css
      /css/lightbox
      /icons
      /images
      /images/design
      /images/fonts
      /images/icon
      /images/portfolio
      /images/portfolio/tooltips
      /images/slider
      /images/thumbs
      /javascript
      /js
```

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.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

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.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2019/03/19

Plugin Output

tcp/443

```
Based on the response to an OPTIONS request :
    - HTTP methods GET HEAD OPTIONS POST are allowed on :

      /
      /css
      /css/lightbox
      /icons
      /images
      /images/design
      /images/fonts
      /images/icon
      /images/portfolio
      /images/portfolio/tooltips
      /images/slider
      /images/thumbs
      /javascript
      /js
```

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

Published: 2000/01/04, Modified: 2019/06/07

Plugin Output

tcp/80

```
The remote web server type is :

Apache/2.4.29 (Ubuntu)
```

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

Published: 2000/01/04, Modified: 2019/06/07

Plugin Output

tcp/443

```
The remote web server type is :

Apache/2.4.29 (Ubuntu)
```

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

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/80

```

Response Code : HTTP/1.1 200 OK

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

  Date: Thu, 14 Nov 2019 21:48:57 GMT
  Server: Apache/2.4.29 (Ubuntu)
  Last-Modified: Thu, 15 Aug 2019 20:21:44 GMT
  ETag: "3514-5902d9f4f2569"
  Accept-Ranges: bytes
  Content-Length: 13588
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<!DOCTYPE html>
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="fr"> <![endif]-->
<!--[if IE 7]>    <html class="no-js ie7 oldie" lang="fr"> <![endif]-->
<!--[if IE 8]>    <html class="no-js ie8 oldie" lang="fr"> <![endif]-->
<!--[if gt IE 8]> <html class="no-js" lang="fr"> <![endif]-->
<html>
```

```
<head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>plantillas web</title>
    <!--BEGIN OF TERMS OF USE. DO NOT EDIT OR DELETE THESE LINES. IF YOU EDIT OR DELETE THESE LINES
 AN ALERT MESSAGE MAY APPEAR WHEN TEMPLATE WILL BE ONLINE-->
    <style>
        #free-flash-header a,
        #free-flash-header a:hover {
            color: #363636;
        }

        #free-flash-header a:hover {
            text-decoration: none
        }
    </style>
    <!--END OF TERMS OF USE-->
    <!-- Bootstrap -->
    <link href="css/reset.css" rel="stylesheet" type="text/css" media="all">
    <link href="css/bootstrap.css" rel="stylesheet" type="text/css" media="all">
    <link href="css/style.css" rel="stylesheet" type="text/css" media="all">
    <link href="css/font.css" rel="stylesheet" type="text/css" media="all">
    <link href="css/mobile.css" rel="stylesheet" type="text/css" media="all">
    <!-- end Bootstrap -->
    <link href='http://fonts.googleapis.com/css?
family=Lato:400,400italic,700,700italic,900,900italic,300italic,300,100italic,100' rel='stylesheet'
 type='text/css'>
    <!-- LightBox -->
    <link href [...]
```

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

Published: 2007/01/30, Modified: 2017/11/13

Plugin Output

tcp/443

```

Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : yes
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

  Date: Thu, 14 Nov 2019 21:48:58 GMT
  Server: Apache/2.4.29 (Ubuntu)
  Last-Modified: Thu, 15 Aug 2019 20:21:44 GMT
  ETag: "3514-5902d9f4f2569"
  Accept-Ranges: bytes
  Content-Length: 13588
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<!DOCTYPE html>
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="fr"> <![endif]-->
<!--[if IE 7]>    <html class="no-js ie7 oldie" lang="fr"> <![endif]-->
<!--[if IE 8]>    <html class="no-js ie8 oldie" lang="fr"> <![endif]-->
<!--[if gt IE 8]> <html class="no-js" lang="fr"> <![endif]-->
<html>
```

```
<head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>plantillas web</title>
    <!--BEGIN OF TERMS OF USE. DO NOT EDIT OR DELETE THESE LINES. IF YOU EDIT OR DELETE THESE LINES
 AN ALERT MESSAGE MAY APPEAR WHEN TEMPLATE WILL BE ONLINE-->
    <style>
        #free-flash-header a,
        #free-flash-header a:hover {
            color: #363636;
        }

        #free-flash-header a:hover {
            text-decoration: none
        }
    </style>
    <!--END OF TERMS OF USE-->
    <!-- Bootstrap -->
    <link href="css/reset.css" rel="stylesheet" type="text/css" media="all">
    <link href="css/bootstrap.css" rel="stylesheet" type="text/css" media="all">
    <link href="css/style.css" rel="stylesheet" type="text/css" media="all">
    <link href="css/font.css" rel="stylesheet" type="text/css" media="all">
    <link href="css/mobile.css" rel="stylesheet" type="text/css" media="all">
    <!-- end Bootstrap -->
    <link href='http://fonts.googleapis.com/css?
family=Lato:400,400italic,700,700italic,900,900italic,300italic,300,100italic,100' rel='stylesheet'
 type='text/css'>
    <!-- LightBox -->
    <link hre [...]
```

106658 - JQuery Detection

Synopsis

The web server on the remote host uses JQuery.

Description

Nessus was able to detect JQuery on the remote host.

See Also

https://jquery.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/07, Modified: 2019/09/25

Plugin Output

tcp/80

```
  URL     : http://165.22.34.38/js/jquery-2.1.3.js
  Version : 2.1.3
```

106658 - JQuery Detection

Synopsis

The web server on the remote host uses JQuery.

Description

Nessus was able to detect JQuery on the remote host.

See Also

https://jquery.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/02/07, Modified: 2019/09/25

Plugin Output

tcp/443

```
  URL     : https://165.22.34.38/js/jquery-2.1.3.js
  Version : 2.1.3
```

50344 - Missing or Permissive Content-Security-Policy frame-ancestors 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) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors 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://www.nessus.org/u?55aa8f57

http://www.nessus.org/u?07cc2a06

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

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

Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2018/11/15

Plugin Output

tcp/80

```

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

  - http://165.22.34.38/
  - http://165.22.34.38/about.htm
  - http://165.22.34.38/contact.htm
  - http://165.22.34.38/contact_message.htm
  - http://165.22.34.38/css/
  - http://165.22.34.38/css/lightbox/
  - http://165.22.34.38/images/
  - http://165.22.34.38/images/design/
  - http://165.22.34.38/images/fonts/
  - http://165.22.34.38/images/icon/
  - http://165.22.34.38/images/portfolio/
```

```
    - http://165.22.34.38/images/portfolio/tooltips/
    - http://165.22.34.38/images/slider/
    - http://165.22.34.38/images/thumbs/
    - http://165.22.34.38/index.htm
    - http://165.22.34.38/js/
    - http://165.22.34.38/news.htm
    - http://165.22.34.38/portfolio.htm
```

50344 - Missing or Permissive Content-Security-Policy frame-ancestors 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) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors 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://www.nessus.org/u?55aa8f57

http://www.nessus.org/u?07cc2a06

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

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

Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2018/11/15

Plugin Output

tcp/443

```

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

  - https://165.22.34.38/
  - https://165.22.34.38/about.htm
  - https://165.22.34.38/contact.htm
  - https://165.22.34.38/contact_message.htm
  - https://165.22.34.38/css/
  - https://165.22.34.38/css/lightbox/
  - https://165.22.34.38/images/
  - https://165.22.34.38/images/design/
  - https://165.22.34.38/images/fonts/
  - https://165.22.34.38/images/icon/
  - https://165.22.34.38/images/portfolio/
```

```
    - https://165.22.34.38/images/portfolio/tooltips/
    - https://165.22.34.38/images/slider/
    - https://165.22.34.38/images/thumbs/
    - https://165.22.34.38/index.htm
    - https://165.22.34.38/js/
    - https://165.22.34.38/news.htm
    - https://165.22.34.38/portfolio.htm
```

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

Published: 2010/10/26, Modified: 2017/05/16

Plugin Output

tcp/80

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

  - http://165.22.34.38/
  - http://165.22.34.38/about.htm
  - http://165.22.34.38/contact.htm
  - http://165.22.34.38/contact_message.htm
  - http://165.22.34.38/css/
  - http://165.22.34.38/css/lightbox/
  - http://165.22.34.38/images/
  - http://165.22.34.38/images/design/
  - http://165.22.34.38/images/fonts/
  - http://165.22.34.38/images/icon/
  - http://165.22.34.38/images/portfolio/
  - http://165.22.34.38/images/portfolio/tooltips/
  - http://165.22.34.38/images/slider/
  - http://165.22.34.38/images/thumbs/
  - http://165.22.34.38/index.htm
  - http://165.22.34.38/js/
```

```
    - http://165.22.34.38/news.htm
    - http://165.22.34.38/portfolio.htm
```

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

Published: 2010/10/26, Modified: 2017/05/16

Plugin Output

tcp/443

```

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

  - https://165.22.34.38/
  - https://165.22.34.38/about.htm
  - https://165.22.34.38/contact.htm
  - https://165.22.34.38/contact_message.htm
  - https://165.22.34.38/css/
  - https://165.22.34.38/css/lightbox/
  - https://165.22.34.38/images/
  - https://165.22.34.38/images/design/
  - https://165.22.34.38/images/fonts/
  - https://165.22.34.38/images/icon/
  - https://165.22.34.38/images/portfolio/
  - https://165.22.34.38/images/portfolio/tooltips/
  - https://165.22.34.38/images/slider/
  - https://165.22.34.38/images/thumbs/
  - https://165.22.34.38/index.htm
  - https://165.22.34.38/js/
```

```
    - https://165.22.34.38/news.htm
    - https://165.22.34.38/portfolio.htm
```

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

Published: 2009/02/04, Modified: 2019/08/20

Plugin Output

tcp/80

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

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

Published: 2009/02/04, Modified: 2019/08/20

Plugin Output

tcp/443

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

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

Published: 2005/08/26, Modified: 2019/03/06

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.8.0
Plugin feed version : 201911132050
Scanner edition used : Nessus Home
Scan type : Normal
Scan policy used : Basic Network Scan
Scanner IP : 10.0.2.15
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 : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : Detected
Allow post-scan editing: Yes
Scan Start Date : 2019/11/14 15:29 CST
Scan duration : 13169 sec
```

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

Published: 2003/12/09, Modified: 2019/09/04

Plugin Output

tcp/0

```
Remote operating system : AIX 5.3
Confidence level : 65
Method : SinFP


The remote host is running AIX 5.3
```

10919 - Open Port Re-check

Synopsis

Previously open ports are now closed.

Description

One of several ports that were previously open are now closed or unresponsive.

There are several possible reasons for this :

- The scan may have caused a service to freeze or stop running.

- An administrator may have stopped a particular service during the scanning process.

This might be an availability problem related to the following :

- A network outage has been experienced during the scan, and the remote network cannot be reached anymore by the scanner.

- This scanner may has been blacklisted by the system administrator or by an automatic intrusion detection / prevention system that detected the scan.

- The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective.

In any case, the audit of the remote host might be incomplete and may need to be done again.

Solution

- Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

Risk Factor

None

Plugin Information

Published: 2002/03/19, Modified: 2014/06/04

Plugin Output

tcp/0

```
Port 443 was detected as being open but is now unresponsive
Port 80 was detected as being open but is now unresponsive
```

50845 - OpenSSL Detection

Synopsis

The remote service appears to use OpenSSL to encrypt traffic.

Description

Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic.

Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366).

See Also

https://www.openssl.org/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/11/30, Modified: 2018/11/15

Plugin Output

tcp/443

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/01, Modified: 2019/03/01

Plugin Output

tcp/443

```
This port supports TLSv1.0/TLSv1.1/TLSv1.2.
```

83298 - SSL Certificate Chain Contains Certificates Expiring Soon

Synopsis

The remote host has an SSL certificate chain with one or more certificates that are going to expire soon.

Description

The remote host has an SSL certificate chain with one or more SSL certificates that are going to expire soon. Failure to renew these certificates before the expiration date may result in denial of service for users.

Solution

Renew any soon to expire SSL certificates.

Risk Factor

None

Plugin Information

Published: 2015/05/08, Modified: 2015/05/08

Plugin Output

tcp/443

```

The following soon to expire certificate was part of the certificate
chain sent by the remote host :

|-Subject   : CN=sitiodepruebas.org
|-Not After : Jan 13 03:28:37 2020 GMT
```

42981 - SSL Certificate Expiry - Future Expiry

Synopsis

The SSL certificate associated with the remote service will expire soon.

Description

The SSL certificate associated with the remote service will expire soon.

Solution

Purchase or generate a new SSL certificate in the near future to replace the existing one.

Risk Factor

None

Plugin Information

Published: 2009/12/02, Modified: 2012/04/02

Plugin Output

tcp/443

```

The SSL certificate will expire within 60 days, at
Jan 13 03:28:37 2020 GMT :

  Subject          : CN=sitiodepruebas.org
  Issuer           : C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
  Not valid before : 5da53ce5
  Not valid after  : Jan 13 03:28:37 2020 GMT
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2008/05/19, Modified: 2019/07/18

Plugin Output

tcp/443

```
Subject Name:

Common Name: sitiodepruebas.org

Issuer Name:

Country: US
Organization: Let's Encrypt
Common Name: Let's Encrypt Authority X3

Serial Number: 03 C6 79 6A EB CD A6 6D 18 A1 61 4B C1 1F B0 5F 1A 7B

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Oct 15 03:28:37 2019 GMT
Not Valid After: Jan 13 03:28:37 2020 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 C4 7F B4 24 7D 06 A8 1C A3 E1 B2 68 93 D1 4A 53 B1 C0 BA
            E4 6A CF FB 01 4C D8 06 36 8A 45 17 51 F9 2E 7D 97 58 8A A2
            59 8E 78 A9 0A 72 EB E4 F8 76 2A BE 59 27 95 C6 B9 1F 2D 83
            FF 74 F7 6C D7 F0 02 C2 CD 7C B9 BD 9E 1B 37 02 D4 C5 4A 47
            2E D2 EE 6A 5B A2 08 42 B5 AE E1 02 62 CE F2 D9 60 17 CF 7B
            D4 27 C3 89 58 44 C8 2C 98 79 3F CC 44 C2 58 FE 7F CF 8D F3
            1F D7 A9 D2 FE 21 9D 01 11 D2 D1 99 27 37 52 57 CA D6 69 FA
            75 4A 79 61 EB 8A 18 5E B3 C8 D1 AA D3 22 24 51 08 0C FE 64
            69 96 EC 2B 44 01 33 F1 51 7F F1 58 BC 1B 24 DB F1 FC 0D EA
            8D 4D 6F C0 93 81 84 82 41 41 98 56 B4 06 68 3B 5D D2 CC AB
            B9 62 96 EB 43 C2 60 84 EC 8C 73 CA 97 FB 0F 8D BA 12 D4 80
            9D 54 65 E7 65 C7 CA 32 22 66 09 14 CF F4 6E 1E 29 DD 66 04
            29 CC AA 7D D1 68 0A 2A A9 06 9A 77 42 F3 F9 C3 5D
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 16 1F 89 40 81 40 AA 69 E1 9C B8 E8 B7 4E E2 52 6B 7F D5
           49 1A A3 1F FF B5 C1 FD B6 22 C6 1C 7B 64 5A 43 17 02 65 E9
           47 B3 9F 25 01 24 EE 92 50 9D 03 79 16 BC E8 83 95 9D 10 81
           02 CC BB 2A 7C 37 95 DE 43 F8 68 B2 C4 A4 A2 98 57 3C B6 73
           5C 82 14 FA FF 9F AC E0 1A D7 E7 51 8D EA DA 27 C4 B7 63 1C
           A1 44 D8 C4 02 61 E5 D2 25 1C B8 DA 26 55 48 5F 39 8A 62 D0
           91 91 AF ED CA 9B 17 6D 5D C9 54 08 EB 1D A1 4A DB 8C F2 6C
           8B 68 3D 48 30 1A A9 8C B6 D4 8E 57 13 51 B7 E0 D0 63 53 FB
           95 5B 6F 91 BF 04 D8 47 01 28  [...]
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Cipher Block Chaining ciphers, which combine previous blocks with subsequent ones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode. These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have the potential to leak information if used improperly.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

http://www.nessus.org/u?cc4a822a

https://www.openssl.org/~bodo/tls-cbc.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/22, Modified: 2018/11/15

Plugin Output

tcp/443

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

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    DHE-RSA-AES128-SHA256        Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    DHE-RSA-AES256-SHA256        Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA256
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384
    RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    RSA-AES256-SHA256            Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA256
```

```
 The fields above are :

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

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

https://www.openssl.org/docs/man1.1.0/apps/ciphers.html

http://www.nessus.org/u?3a040ada

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2006/06/05, Modified: 2019/05/10

Plugin Output

tcp/443

```
Here is the list of SSL ciphers supported by the remote server :
Each group is reported per SSL Version.

SSL Version : TLSv12
  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA256        Kx=DH          Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    DHE-RSA-AES256-SHA384        Kx=DH          Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-CHACHA20-POLY1305  Kx=ECDH        Au=RSA      Enc=ChaCha20-Poly1305(256)  Mac=SHA256
    RSA-AES128-SHA256            Kx=RSA         Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    RSA-AES256-SHA384            Kx=RSA         Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    AES128-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    AES256-SHA                   Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    DHE-RSA-AES128-SHA256        Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    DHE-RSA-AES256-SHA256        Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA256
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384
    RSA-AES128-SHA256             Kx=RSA         Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    RSA-AES256-SHA256             Kx=RSA         Au=RSA      Enc=AES-CBC(256)         Mac=SHA256


SSL Version : TLSv [...]
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

The remote service supports the use of SSL Perfect Forward Secrecy ciphers, which maintain confidentiality even if the key is stolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption. These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server's private key is compromised.

See Also

https://www.openssl.org/docs/manmaster/man1/ciphers.html

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/12/07, Modified: 2018/11/15

Plugin Output

tcp/443

```

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

  High Strength Ciphers (>= 112-bit key)

    DHE-RSA-AES128-SHA256        Kx=DH          Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    DHE-RSA-AES256-SHA384        Kx=DH          Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-GCM(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-GCM(256)         Mac=SHA384
    ECDHE-RSA-CHACHA20-POLY1305  Kx=ECDH        Au=RSA      Enc=ChaCha20-Poly1305(256)  Mac=SHA256
    DHE-RSA-AES128-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    DHE-RSA-AES256-SHA           Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    ECDHE-RSA-AES128-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA1
    ECDHE-RSA-AES256-SHA         Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA1
    DHE-RSA-AES128-SHA256        Kx=DH          Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    DHE-RSA-AES256-SHA256        Kx=DH          Au=RSA      Enc=AES-CBC(256)         Mac=SHA256
    ECDHE-RSA-AES128-SHA256      Kx=ECDH        Au=RSA      Enc=AES-CBC(128)         Mac=SHA256
    ECDHE-RSA-AES256-SHA384      Kx=ECDH        Au=RSA      Enc=AES-CBC(256)         Mac=SHA384
```

```
The fields above are :

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

94761 - SSL Root Certification Authority Certificate Information

Synopsis

A root Certification Authority certificate was found at the top of the certificate chain.

Description

The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain.

See Also

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)

Solution

Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2016/11/14, Modified: 2018/11/15

Plugin Output

tcp/443

```

The following root Certification Authority certificate was found :

|-Subject             : O=Digital Signature Trust Co./CN=DST Root CA X3
|-Issuer              : O=Digital Signature Trust Co./CN=DST Root CA X3
|-Valid From          : Sep 30 21:12:19 2000 GMT
|-Valid To            : Sep 30 14:01:15 2021 GMT
|-Signature Algorithm : SHA-1 With RSA Encryption
```

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

Published: 2007/08/19, Modified: 2019/10/29

Plugin Output

tcp/80

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

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

Published: 2007/08/19, Modified: 2019/10/29

Plugin Output

tcp/443

```
A TLSv1 server answered on this port.
```

tcp/443

```
A web server is running on this port through TLSv1.
```

84821 - TLS ALPN Supported Protocol Enumeration

Synopsis

The remote host supports the TLS ALPN extension.

Description

The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports.

See Also

https://tools.ietf.org/html/rfc7301

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2015/07/17, Modified: 2016/02/15

Plugin Output

tcp/443

```
ALPN Supported Protocols:

  http/1.1
```

104743 - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.1 and 1.2 are designed against these flaws and should be used whenever possible.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution

Enable support for TLS 1.1 and 1.2, and disable support for TLS 1.0.

Risk Factor

None

Plugin Information

Published: 2017/11/22, Modified: 2018/07/11

Plugin Output

tcp/443

```
TLSv1 is enabled and the server supports at least one cipher.
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.1.

TLS 1.1 lacks support for current and recommended cipher suites.

Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1

PCI DSS v3.2 still allows TLS 1.1 as of June 30, 2018, but strongly recommends the use of TLS 1.2. A proposal is currently before the IETF to fully deprecate TLS 1.1 and many vendors have already proactively done this.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

http://www.nessus.org/u?c8ae820d

Solution

Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Risk Factor

None

Plugin Information

Published: 2019/01/08, Modified: 2019/01/08

Plugin Output

tcp/443

```
TLSv1.1 is enabled and the server supports at least one cipher.
```

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

Published: 1999/11/27, Modified: 2019/03/06

Plugin Output

udp/0

```
For your information, here is the traceroute from 10.0.2.15 to 165.22.34.38 :
10.0.2.15
10.0.2.2
165.22.34.38

Hop Count: 2
```

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

Published: 2016/06/24, Modified: 2016/06/24

Plugin Output

tcp/80

```

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

  - http://165.22.34.38/
  - http://165.22.34.38/about.htm
  - http://165.22.34.38/contact.htm
  - http://165.22.34.38/contact_message.htm
  - http://165.22.34.38/css/
  - http://165.22.34.38/css/bootstrap.css
  - http://165.22.34.38/css/font.css
  - http://165.22.34.38/css/lightbox/
  - http://165.22.34.38/css/lightbox/style-gallery.css
  - http://165.22.34.38/css/lightbox/style.css
  - http://165.22.34.38/css/lightbox/visuallightbox.css
  - http://165.22.34.38/css/lightbox/vlightbox.css
  - http://165.22.34.38/css/mobile.css
  - http://165.22.34.38/css/reset.css
  - http://165.22.34.38/css/style.css
  - http://165.22.34.38/images/
  - http://165.22.34.38/images/about-me.png
  - http://165.22.34.38/images/about1.png
  - http://165.22.34.38/images/about2.png
  - http://165.22.34.38/images/design/
  - http://165.22.34.38/images/design/borderBottomCenter.png
  - http://165.22.34.38/images/design/borderBottomLeft.png
```

```
    - http://165.22.34.38/images/design/borderBottomRight.png
    - http://165.22.34.38/images/design/borderMiddleLeft.png
    - http://165.22.34.38/images/design/borderMiddleRight.png
    - http://165.22.34.38/images/design/borderTopCenter.png
    - http://165.22.34.38/images/design/borderTopLeft.png
    - http://165.22.34.38/images/design/borderTopRight.png
    - http://165.22.34.38/images/design/close.gif
    - http://165.22.34.38/images/design/closelabel.gif
    - http://165.22.34.38/images/design/loading.gif
    - http://165.22.34.38/images/design/next.png
    - http://165.22.34.38/images/design/next_ie6.gif
    - http://165.22.34.38/images/design/nextlabel.gif
    - http://165.22.34.38/images/design/pause.gif
    - http://165.22.34.38/images/design/prev.png
    - http://165.22.34.38/images/design/prev_ie6.gif
    - http://165.22.34.38/images/design/prevlabel.gif
    - http://165.22.34.38/images/design/start.gif
    - http://165.22.34.38/images/fonts/
    - http://165.22.34.38/images/fonts/fullscreen.eot
    - http://165.22.34.38/images/fonts/fullscree [...]
```

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

Published: 2016/06/24, Modified: 2016/06/24

Plugin Output

tcp/443

```

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

  - https://165.22.34.38/
  - https://165.22.34.38/about.htm
  - https://165.22.34.38/contact.htm
  - https://165.22.34.38/contact_message.htm
  - https://165.22.34.38/css/
  - https://165.22.34.38/css/bootstrap.css
  - https://165.22.34.38/css/font.css
  - https://165.22.34.38/css/lightbox/
  - https://165.22.34.38/css/lightbox/style-gallery.css
  - https://165.22.34.38/css/lightbox/style.css
  - https://165.22.34.38/css/lightbox/visuallightbox.css
  - https://165.22.34.38/css/lightbox/vlightbox.css
  - https://165.22.34.38/css/mobile.css
  - https://165.22.34.38/css/reset.css
  - https://165.22.34.38/css/style.css
  - https://165.22.34.38/images/
  - https://165.22.34.38/images/about-me.png
  - https://165.22.34.38/images/about1.png
  - https://165.22.34.38/images/about2.png
  - https://165.22.34.38/images/design/
  - https://165.22.34.38/images/design/borderBottomCenter.png
  - https://165.22.34.38/images/design/borderBottomLeft.png
```

```
    - https://165.22.34.38/images/design/borderBottomRight.png
    - https://165.22.34.38/images/design/borderMiddleLeft.png
    - https://165.22.34.38/images/design/borderMiddleRight.png
    - https://165.22.34.38/images/design/borderTopCenter.png
    - https://165.22.34.38/images/design/borderTopLeft.png
    - https://165.22.34.38/images/design/borderTopRight.png
    - https://165.22.34.38/images/design/close.gif
    - https://165.22.34.38/images/design/closelabel.gif
    - https://165.22.34.38/images/design/loading.gif
    - https://165.22.34.38/images/design/next.png
    - https://165.22.34.38/images/design/next_ie6.gif
    - https://165.22.34.38/images/design/nextlabel.gif
    - https://165.22.34.38/images/design/pause.gif
    - https://165.22.34.38/images/design/prev.png
    - https://165.22.34.38/images/design/prev_ie6.gif
    - https://165.22.34.38/images/design/prevlabel.gif
    - https://165.22.34.38/images/design/start.gif
    - https://165.22.34.38/images/fonts/
    - https://165.22.34.38/images/fonts/fullscreen.eot
    - h [...]
```

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/w/page/13246953/Predictable%20Resource%20Location

Solution

n/a

Risk Factor

None

References

XREF	OWASP:OWASP-CM-006

Plugin Information

Published: 2002/06/26, Modified: 2018/11/15

Plugin Output

tcp/80

```
The following directories were discovered:
/css, /icons, /images, /javascript, /js

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
```

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/w/page/13246953/Predictable%20Resource%20Location

Solution

n/a

Risk Factor

None

References

XREF	OWASP:OWASP-CM-006

Plugin Information

Published: 2002/06/26, Modified: 2018/11/15

Plugin Output

tcp/443

```
The following directories were discovered:
/css, /icons, /images, /javascript, /js

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
```

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

Published: 2001/05/04, Modified: 2019/08/20

Plugin Output

tcp/80

```

Webmirror performed 134 queries in 106s (1.0264 queries per second)

The following CGIs have been discovered :


+ CGI : /contact.php
  Methods : POST
  Argument : email
  Argument : message
  Argument : name
  Argument : subject
  Argument : telephone

Directory index found at /js/
Directory index found at /images/
Directory index found at /css/
Directory index found at /css/lightbox/
Directory index found at /images/design/
Directory index found at /images/fonts/
Directory index found at /images/icon/
Directory index found at /images/portfolio/
Directory index found at /images/slider/
Directory index found at /images/thumbs/
Directory index found at /images/portfolio/tooltips/
```

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

Published: 2001/05/04, Modified: 2019/08/20

Plugin Output

tcp/443

```

Webmirror performed 134 queries in 133s (1.007 queries per second)

The following CGIs have been discovered :


+ CGI : /contact.php
  Methods : POST
  Argument : email
  Argument : message
  Argument : name
  Argument : subject
  Argument : telephone

Directory index found at /js/
Directory index found at /images/
Directory index found at /css/
Directory index found at /css/lightbox/
Directory index found at /images/design/
Directory index found at /images/fonts/
Directory index found at /images/icon/
Directory index found at /images/portfolio/
Directory index found at /images/slider/
Directory index found at /images/thumbs/
Directory index found at /images/portfolio/tooltips/
```