Thank you for taking the time to review this sample raw report! More about PEN Consultants and our services can be found at: https://penconsultants.com/whyPENConsultants.

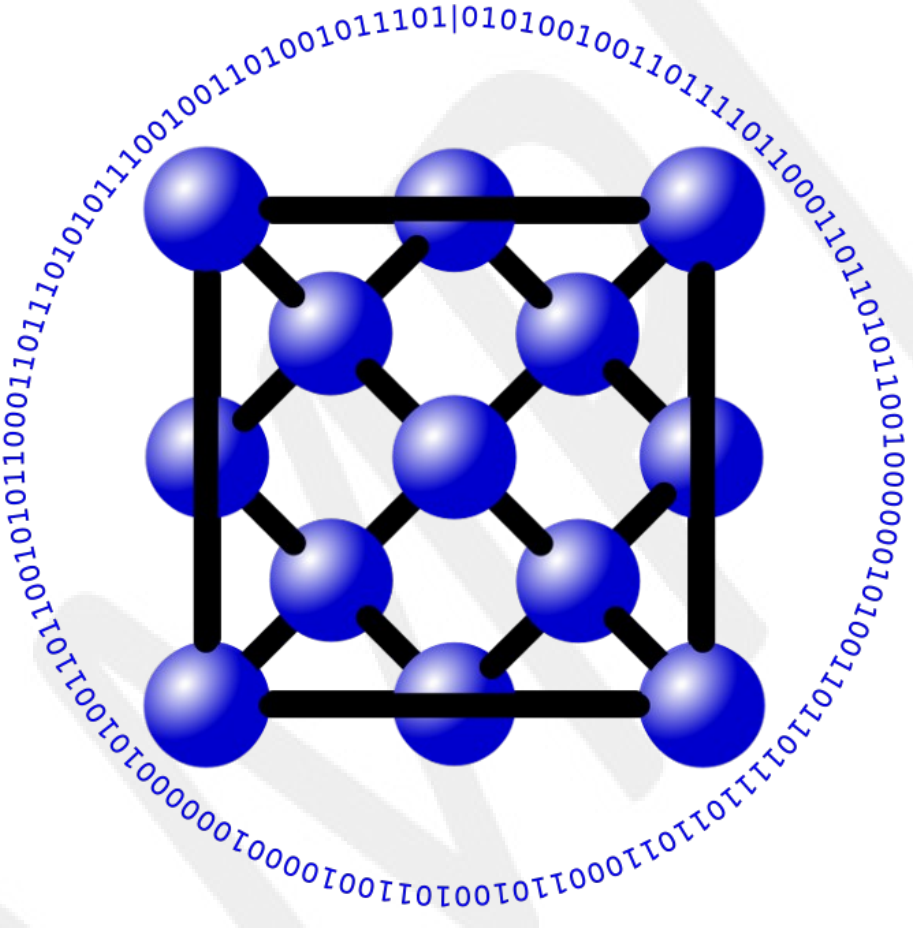
Please let us know if you are interested in learning more, have questions, or are ready for us to serve your security testing needs.

PEN Consultants
Phone: 830-446-3411
Email: info@PENConsultants.com

DISCLAIMER: This is a sample of a RAW scanner report. See https://penconsultants.com/reportingLevels for other reporting options we provide.

PEN Consultants

Information & Cybersecurity Testing Services



Security Testing

Raw Scanner Report

Acme Corporation

PEN Consultants, LLC
13423 Blanco Rd #3124
San Antonio, TX 78216
https://penconsultants.com

March 25, 2019

Acme Corporation,

Your organization requested PEN Consultants to perform security testing against one or more of your applications, systems, networks, or facilities to assess your current security posture. We are honored to have been trusted to serve your organization with your information and cybersecurity needs.

Please read through this document in its entirety, and return it to us at your earliest convenience with any questions or requested changes. Alternatively, a conference call can be setup to work through the document.

A detailed explanation of our services can be found at https://PENConsultants.com/services.

The general timeline for the engagement is as follows:

- Phase 1 - Pre-testing
  - Request for services, initial phone/email discussions, etc. (COMPLETE)
  - Mutual Non-Disclosure Agreement (COMPLETE)
  - Discuss and define scope, goals, objectives, etc. (COMPLETE)
  - Preliminary Service Quote (COMPLETE)
  - Scoping Questionnaire (COMPLETE)
  - Service Contract and Statement Of Work (SOW), to ensure all parties understand what our service provides (COMPLETE)
  - Kick-off document, with initial change requests needed prior to scheduling testing (COMPLETE)
- Phase 2 - Testing
  - Testing and evaluation, as defined in the SOW (COMPLETE)
  - Red Teaming only: Once all objectives above are met, we'll coordinate with you to go into the "getting noisy" phase (if applicable/requested) (N/A)
- Phase 3 – Reporting
  - Deliver raw vulnerability scanner report(s) in fulfillment of the SOW, send invoice, and schedule an exit interview (THIS DOCUMENT)
- Phase 4 – Post-Testing
  - Optional phases - can be purchased/added at anytime:
    - Brief the report to IT support staff, leadership, or 3rd parties
    - Assist IT support staff in implementing and verifying recommended mitigations
    - Post remediation testing and updated reporting
    - Begin Cybersecurity Unlimited retainer service
    - Schedule quarterly testing

Sample Vulnerability Scan Report

Mon, 18 Mar 2019 19:22:47 CDT

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

192.168.2.47

CRITICAL	HIGH	MEDIUM	LOW	INFO
1	1	6	1	29

Scan Information

Start time:	Mon Mar 18 19:19:30 2019
End time:	Mon Mar 18 19:22:47 2019

Host Information

DNS Name:	vulnerable.home.lan
IP:	192.168.2.47
MAC Address:	00:08:14:27:98:17
OS:	Linux Kernel 3.10, Linux Kernel 3.13, Linux Kernel 4.2, Linux Kernel 4.8

Vulnerabilities

84729 - Microsoft Windows Server 2003 Unsupported Installation Detection -

Synopsis

The remote operating system is no longer supported.

Description

The remote host is running Microsoft Windows Server 2003. Support for this operating system by Microsoft ended July 14th, 2015.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.

See Also

http://www.nessus.org/u?76f71a39
http://www.nessus.org/u?321523eb
https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
http://www.nessus.org/u?8dcab5e4

Solution

Upgrade to a version of Windows that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

9.0 (CVSS:3.0/E:P/RL:O/RC:C)

CVSS Base Score

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

CVSS Temporal Score

7.8 (CVSS2#E:POC/RL:OF/RC:C)

References

XREF EDB-ID:41929

Plugin Information

Published: 2015/07/14, Modified: 2018/11/15

Plugin Output

tcp/0

20007 - SSL Version 2 and 3 Protocol Detection -

Synopsis

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

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf
http://www.nessus.org/u?b06c7e95
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/ssl-poodle.pdf
http://www.nessus.org/u?5d15ba70
https://www.imperialviolet.org/2014/10/14/poodle.html
https://tools.ietf.org/html/rfc7507
https://tools.ietf.org/html/rfc7568

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.1 (with approved cipher suites) or higher instead.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS Base Score

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

Plugin Information

Published: 2005/10/12, Modified: 2019/02/27

Plugin Output

tcp/443

```
- SSLv2 is enabled and the server supports at least one cipher.

Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

DES-CBC3-MD5 Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=MD5

High Strength Ciphers (>= 112-bit key)

RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5

The fields above are :

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

- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

DES-CBC3-SHA Kx=RSA Au=RSA Enc=3DES-CBC(168) Mac=SHA1

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
RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1

The fields above are :

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

122235 - Apache Struts Config Browser Plugin Detection -

Synopsis

Detects Apache Struts Config Browser Plugin on the remote host.

Description

The Apache Struts Config Browser Plugin, a simple tool to help view an application's configuration at runtime, was detected on the remote host.

This plugin should be used only during development phase and access to it should be strictly restricted.

See Also

https://struts.apache.org/plugins/config-browser/

Solution

Ensure proper restrictions are in place, or remove the Config Browser Plugin if it is not required.

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: 2019/02/15, Modified: 2019/03/06

Plugin Output

tcp/80

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

Version : 2.5.12
URL : http://vulnerable.home.lan/config-browser/
```

12085 - Apache Tomcat Default Files -

Synopsis

The remote web server contains default files.

Description

The default error page, default index page, example JSPs, and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself.

See Also

https://wiki.apache.org/tomcat/FAQ/Miscellaneous#Q6
https://www.owasp.org/index.php/Securing_tomcat

Solution

Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

References

XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information:

Published: 2004/03/02, Modified: 2018/01/30

Plugin Output

tcp/80

```
The following default files were found :

/nessus-check/default-404-error-page.html
```

11411 - Backup Files Disclosure -

Synopsis

It is possible to retrieve file backups from the remote web server.

Description

By appending various suffixes (ie: .old, .bak, ~, etc...) to the names of various files on the remote host, it seems possible to retrieve their contents, which may result in disclosure of sensitive information.

See Also

http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location

Solution

Ensure the files do not contain any sensitive information, such as credentials to connect to a database, and delete or protect those files that should not be accessible.

Risk Factor

Medium

CVSS Base Score

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

Plugin Information:

Published: 2003/03/17, Modified: 2018/11/15

Plugin Output

tcp/80

```
It is possible to read the following backup files :

- File : /orders/3~
URL : http://vulnerable.home.lan/orders/3~

- File : /orders/4~
URL : http://vulnerable.home.lan/orders/4~

- File : /orders/5~
URL : http://vulnerable.home.lan/orders/5~
```

57608 - SMB Signing not required -

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/help/887429/overview-of-server-message-block-signing
http://technet.microsoft.com/en-us/library/cc731957.aspx
http://www.nessus.org/u?74b80723
https://www.samba.org/samba/docs/current/man-html/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 v3.0 Base Score

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

CVSS v3.0 Temporal Score

4.6 (CVSS:3.0/E:U/RL:O/RC:C)

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:

Published: 2012/01/19, Modified: 2018/11/15

Plugin Output

tcp/445

118154 - SSH Protocol Authentication Bypass (Remote Exploit Check) -

Synopsis

The remote server is vulnerable to an authentication bypass.

Description

The remote ssh server is vulnerable to an authentication bypass. An attacker can bypass authentication by presenting SSH2_MSG_USERAUTH_SUCCESS message in place of the SSH2_MSG_USERAUTH_REQUEST method that normally would initiate authentication.

Note: This vulnerability was disclosed in a libssh advisory but has also been observed as applicable to other applications and software packages.

See Also

http://www.nessus.org/u?6f6b157e
http://www.nessus.org/u?505261f8
http://www.nessus.org/u?58a0f73d

Solution

Upgrade to libssh 0.7.6 / 0.8.4 or later, if applicable. Otherwise, contact your product vendor.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

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

STIG Severity

I

References

BID	105677
BID	106762
CVE	CVE-2018-10933
CVE	CVE-2018-1000805
XREF	IAVA:2018-A-0347

Plugin Information:

Published: 2018/10/17, Modified: 2019/02/07

Plugin Output

tcp/22

```
Nessus was able to successfully open a channel on the libssh server
with no credentials.
```

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://vulnerable.home.lan/orders/3/deleteConfirm
- http://vulnerable.home.lan/orders/3/edit
- http://vulnerable.home.lan/orders/4/deleteConfirm
- http://vulnerable.home.lan/orders/4/edit
- http://vulnerable.home.lan/orders/5/deleteConfirm
- http://vulnerable.home.lan/orders/5/edit
- http://vulnerable.home.lan/orders/new
```

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

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

References

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

Plugin Information:

Published: 2013/10/28, Modified: 2018/07/30

Plugin Output

tcp/22

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

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc

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

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
```

39446 - Apache Tomcat Detection -

Synopsis

The remote web server is an Apache Tomcat server.

Description

Nessus was able to detect a remote Apache Tomcat web server.

See Also

https://tomcat.apache.org/

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/06/18, Modified: 2019/01/11

Plugin Output

tcp/80

```
URL : http://vulnerable.home.lan/
Version : 6.0.41
backported : 1
source : Apache Tomcat/6.0.41
```

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:

Published: 2009/06/25, Modified: 2015/07/07

Plugin Output

tcp/80

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

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:

Published: 2010/07/26, Modified: 2017/01/05

Plugin Output

tcp/80

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

+ The following resources may be vulnerable to injectable parameter :

+ The 'amount' parameter of the /orders CGI :

/orders?amount=%00kkzveu

-------- output --------
<td>3</td>
<td>Bob</td>
<td>.kkzveu</td>
<td>
<div class="btn-group">
------------------------

+ The 'amount' parameter of the /orders/3 CGI :

/orders/3?amount=%00kkzveu

-------- output --------
<tr>
<td class="span3">Amount</td>
<td class="span9">.kkzveu</td>
</tr>
</table>
------------------------

+ The 'amount' parameter of the /orders/4 CGI :

/orders/4?amount=%00kkzveu

-------- output --------
<tr>
<td class="span3">Amount</td>
<td class="span9">.kkzveu</td>
</tr>
</table>
------------------------

+ The 'amount' parameter of the /orders/5 CGI :

/orders/5?amount=%00kkzveu

-------- output --------
<tr>
<td class="span3">Amount</td>
<td class="span9">.kkzveu</td>
</tr>
</table>
------------------------

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

http://vulnerable.home.lan/orders?amount=%00kkzveu
http://vulnerable.home.lan/orders/3?amount=%00kkzveu
http://vulnerable.home.lan/orders/4?amount=%00kkzveu
http://vulnerable.home.lan/orders/5?amount=%00kkzveu
```

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:

Published: 2009/10/26, Modified: 2014/03/12

Plugin Output

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=4 SP=4 AP=4 SC=4 AC=4
SQL injection : S=336 SP=360 AP=360 SC=360 AC=360
unseen parameters : S=490 SP=525 AP=525 SC=525 AC=525
local file inclusion : S=14 SP=15 AP=15 SC=15 AC=15
web code injection : S=14 SP=15 AP=15 SC=15 AC=15
XML injection : S=14 SP=15 AP=15 SC=15 AC=15
format string : S=28 SP=30 AP=30 SC=30 AC=30
script injection : S=4 SP=4 AP=4 SC=4 AC=4
cross-site scripting (comprehensive test): S=56 SP=60 AP=60 SC=60 AC=60
injectable parameter : S=28 SP=30 AP=30 SC=30 AC=30
cross-site scripting (extended patterns) : S=24 SP=24 AP=24 SC=24 AC=24
directory traversal (write access) : S=28 SP=30 AP=30 SC=30 AC=30
SSI injection : S=42 SP=45 AP=45 SC=45 AC=45
header injection : S=8 SP=8 AP=8 SC=8 AC=8
HTML injection : S=20 SP=20 AP=20 SC=20 AC=20
directory traversal : S=350 SP=375 AP=375 SC=375 AC=375
arbitrary command execution (time based) : S=84 SP=90 AP=90 SC=90 AC=90
persistent XSS : S=56 SP=60 AP=60 SC=60 AC=60
SQL injection (2nd order) : S=14 SP=15 AP=15 SC=15 AC=15
directory traversal (extended test) : S=714 SP=765 AP=765 SC=765 AC=765
arbitrary command execution : S=224 SP=240 AP=240 SC=240 AC=240
blind SQL injection (4 requests) : S=56 SP=60 AP=60 SC=60 AC=60
HTTP response splitting : S=36 SP=36 AP=36 SC=36 AC=36
blind SQL injection : S=168 SP=180 AP=180 SC=180 AC=180

All tests : S=2812 SP=3006 AP=3006 SC=3006 AC=3006

Here are the estimated number of requests in miscellaneous modes
for both methods (GET and POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

on site request forgery : S=8 SP=8 AP=8 SC=8 AC=8
SQL injection : S=672 SP=720 AP=720 SC=720 AC=720
unseen parameters : S=980 SP=1050 AP=1050 SC=1050 AC=1050
local file inclusion : S=28 SP=30 AP=30 SC=30 AC=30
web code injection : S=28 SP=30 AP=30 SC=30 AC=30
XML injection : S=28 SP=30 AP=30 SC=30 AC=30
format string : S=56 SP=60 AP=60 SC=60 AC=60
script injection : S=8 SP=8 AP=8 SC=8 AC=8
cross-site scripting (comprehensive test): S=112 SP=120 AP=120 SC=120 AC=120
injectable parameter : S=56 SP=60 AP=60 SC=60 AC=60
cross-site scripting (extended patterns) : S=48 SP=48 AP=48 SC=48 AC=48
directory traversal (write access) : S=56 SP=60 AP=60 SC=60 AC=60
SSI injection : S=84 SP=90 AP=90 SC=90 AC=90
header injection : S=16 SP=16 AP=16 SC=16 AC=16
HTML injection : S=40 SP=40 AP=40 SC=40 AC=40
directory traversal : S=700 SP=750 AP=750 SC=750 AC=750
arbitrary command execution (time based) : S=168 SP=180 AP=180 SC=180 AC=180
persistent XSS : S=112 SP=120 AP=120 SC=120 AC=120
SQL injection (2nd order) : S=28 SP=30 AP=30 SC=30 AC=30
directory traversal (extended test) : S=1428 SP=1530 AP=1530 SC=1530 AC=1530
arbitrary command execution : S=448 SP=480 AP=480 SC=480 AC=480
blind SQL injection (4 requests) : S=112 SP=120 AP=120 SC=120 AC=120
HTTP response splitting : S=72 SP=72 AP=72 SC=72 AC=72
blind SQL injection : S=336 SP=360 AP=360 SC=360 AC=360

All tests : S=5624 SP=6012 AP=6012 SC=6012 AC=6012

Your mode : single, GET or POST.
Maximum number of requests : 2812
```

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, Modified: 2017/06/06

Plugin Output

tcp/0

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

cpe:/o:linux:linux_kernel:3.10
cpe:/o:linux:linux_kernel:3.13
cpe:/o:linux:linux_kernel:4.2
cpe:/o:linux:linux_kernel:4.8
```

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 : 59
```

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

https://standards.ieee.org/faqs/regauth.html
http://www.nessus.org/u?794673b4

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2009/02/19, Modified: 2018/11/15

Plugin Output

tcp/0

```
The following card manufacturers were identified :

00:08:14:27:98:17 : PCS Systemtechnik GmbH
```

86420 - Ethernet MAC Addresses -

Synopsis

This plugin gathers MAC addresses from various sources and consolidates them into a list.

Description

This plugin gathers MAC addresses discovered from both remote probing of the host (e.g. SNMP and Netbios) and from running local checks (e.g. ifconfig). It then consolidates the MAC addresses into a single, unique, and uniform list.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2015/10/16, Modified: 2018/08/13

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
- 00:08:14:27:98:17
```

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.

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: 2019/03/05

Plugin Output

tcp/80

```
Based on tests of each method :

- HTTP methods GET HEAD OPTIONS POST are allowed on :

/
/css
/orders
/orders/3
/orders/4
/orders/5
```

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: 2019/01/29

Plugin Output

tcp/80

```
The remote web server type is :

Apache-Coyote/1.1
```

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

Synopsis

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

Description

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Published: 2004/02/11, Modified: 2017/04/14

Plugin Output

tcp/0

```
192.168.2.47 resolves as vulnerable.home.lan.
```

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/1.1 303 See Other

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

Date: Mon, 18 Mar 2019 16:21:03 GMT
Server: Apache-Coyote/1.1
ETag: 26730913
Location: /orders.xhtml
Content-Language: en
Content-Length: 13
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/plain

Response Body :

/orders.xhtml
```

91634 - HyperText Transfer Protocol (HTTP) Redirect Information -

Synopsis

The remote web server redirects requests to the root directory.

Description

The remote web server issues an HTTP redirect when requesting the root directory of the web server.

This plugin is informational only and does not denote a security problem.

Solution

Analyze the redirect(s) to verify that this is valid operation for your web server and/or application.

Risk Factor

None

Plugin Information:

Published: 2016/06/16, Modified: 2017/10/12

Plugin Output

tcp/80

```
Request : http://vulnerable.home.lan/
HTTP response : HTTP/1.1 303 See Other
Redirect to : http://vulnerable.home.lan/orders.xhtml
Redirect type : 30x redirect

Final page : http://vulnerable.home.lan/orders.xhtml
HTTP response : HTTP/1.1 200 OK
```

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	CWE:200

Plugin Information:

Published: 1999/08/01, Modified: 2019/03/06

Plugin Output

icmp/0

```
The difference between the local and remote clocks is 2 seconds.
```

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://vulnerable.home.lan/orders
- http://vulnerable.home.lan/orders.xhtml
- http://vulnerable.home.lan/orders/3
- http://vulnerable.home.lan/orders/3/deleteConfirm
- http://vulnerable.home.lan/orders/3/edit
- http://vulnerable.home.lan/orders/4
- http://vulnerable.home.lan/orders/4/deleteConfirm
- http://vulnerable.home.lan/orders/4/edit
- http://vulnerable.home.lan/orders/5
- http://vulnerable.home.lan/orders/5/deleteConfirm
- http://vulnerable.home.lan/orders/5/edit
- http://vulnerable.home.lan/orders/new
```

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://vulnerable.home.lan/orders
- http://vulnerable.home.lan/orders.xhtml
- http://vulnerable.home.lan/orders/3
- http://vulnerable.home.lan/orders/3/deleteConfirm
- http://vulnerable.home.lan/orders/3/edit
- http://vulnerable.home.lan/orders/4
- http://vulnerable.home.lan/orders/4/deleteConfirm
- http://vulnerable.home.lan/orders/4/edit
- http://vulnerable.home.lan/orders/5
- http://vulnerable.home.lan/orders/5/deleteConfirm
- http://vulnerable.home.lan/orders/5/edit
- http://vulnerable.home.lan/orders/new
```

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: 2019/03/06

Plugin Output

tcp/80

```
Port 80/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 : 8.2.3
Plugin feed version : 201903151842
Scanner edition used : Nessus
Scan type : Normal
Scan policy used : Advanced Scan
Scanner IP : 192.168.2.43
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 : 2019/3/18 11:19 CDT
Scan duration : 193 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: 2019/01/10

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 3.10
Linux Kernel 3.13
Linux Kernel 4.2
Linux Kernel 4.8
```

```
Confidence level : 59
Method : SinFP


The remote host is running one of these operating systems :
Linux Kernel 3.10
Linux Kernel 3.13
Linux Kernel 4.2
Linux Kernel 4.8
```

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: 2019/02/22

Plugin Output

tcp/80

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

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:

Published: 2007/05/16, Modified: 2019/03/06

Plugin Output

tcp/0

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 192.168.2.43 to 192.168.2.47 :
192.168.2.43
192.168.2.47

Hop Count: 1
```

85601 - Web Application Cookies Not Marked HttpOnly -

Synopsis

HTTP session cookies might be vulnerable to cross-site scripting attacks.

Description

The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, one or more of those cookies are not marked 'HttpOnly', meaning that a malicious client-side script, such as JavaScript, could read them. The HttpOnly flag is a security mechanism to protect against cross-site scripting attacks, which was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers now support it.

Note that this plugin detects all general cookies missing the HttpOnly cookie flag, whereas plugin 48432 (Web Application Session Cookies Not Marked HttpOnly) will only detect session cookies from an authenticated session missing the HttpOnly cookie flag.

See Also

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

Solution

Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision.

If possible, add the 'HttpOnly' attribute to all session cookies and any cookies containing sensitive data.

Risk Factor

None

References

XREF	CWE:20
XREF	CWE:74
XREF	CWE:79
XREF	CWE:442
XREF	CWE:629
XREF	CWE:711
XREF	CWE:712
XREF	CWE:722
XREF	CWE:725
XREF	CWE:750
XREF	CWE:751
XREF	CWE:800
XREF	CWE:801
XREF	CWE:809
XREF	CWE:811
XREF	CWE:864
XREF	CWE:900
XREF	CWE:928
XREF	CWE:931
XREF	CWE:990

Plugin Information:

Published: 2015/08/24, Modified: 2015/08/24

Plugin Output

tcp/80

```
The following cookie does not set the HttpOnly cookie flag :

Name : JSESSIONID
Path : /
Value : 7F466769908CDA9058CFBB3DC992173A
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

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:

Published: 2015/08/24, Modified: 2015/08/24

Plugin Output

tcp/80

```
The following cookie does not set the secure cookie flag :

Name : JSESSIONID
Path : /
Value : 7F466769908CDA9058CFBB3DC992173A
Domain :
Version : 1
Expires :
Comment :
Secure : 0
Httponly : 0
Port :
```

40773 - Web Application Potentially Sensitive CGI Parameter Detection -

Synopsis

An application was found that may use CGI parameters to control sensitive information.

Description

According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. These parameters should be examined to determine what type of data is controlled and if it poses a security risk.

** This plugin only reports information that may be useful for auditors
** or pen-testers, not a real flaw.

Solution

Ensure sensitive data is not disclosed by CGI parameters. In addition, do not use CGI parameters to control access to resources or privileges.

Risk Factor

None

Plugin Information:

Published: 2009/08/25, Modified: 2012/08/17

Plugin Output

tcp/80

```
Potentially sensitive parameters for CGI /orders/3 :

id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /orders/4 :

id : Potential horizontal or vertical privilege escalation

Potentially sensitive parameters for CGI /orders/5 :

id : Potential horizontal or vertical privilege escalation
```

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://vulnerable.home.lan/css/app.css
- http://vulnerable.home.lan/css/bootstrap.min.css
- http://vulnerable.home.lan/orders
- http://vulnerable.home.lan/orders.xhtml
- http://vulnerable.home.lan/orders/3
- http://vulnerable.home.lan/orders/3/deleteConfirm
- http://vulnerable.home.lan/orders/3/edit
- http://vulnerable.home.lan/orders/4
- http://vulnerable.home.lan/orders/4/deleteConfirm
- http://vulnerable.home.lan/orders/4/edit
- http://vulnerable.home.lan/orders/5
- http://vulnerable.home.lan/orders/5/deleteConfirm
- http://vulnerable.home.lan/orders/5/edit
- http://vulnerable.home.lan/orders/new

Attached is a copy of the sitemap file.
```

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:
/orders

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: 2019/03/06

Plugin Output

tcp/80

```
Webmirror performed 17 queries in 1s (17.000 queries per second)

The following CGIs have been discovered :


+ CGI : /orders/3
Methods : POST
Argument : _method
Value: DELETE
Argument : amount
Value: 33
Argument : clientName
Value: Bob
Argument : id
Value: 3


+ CGI : /orders/4
Methods : POST
Argument : _method
Value: DELETE
Argument : amount
Value: 44
Argument : clientName
Value: Sarah
Argument : id
Value: 4


+ CGI : /orders/5
Methods : POST
Argument : _method
Value: DELETE
Argument : amount
Value: 66
Argument : clientName
Value: Jim
Argument : id
Value: 5


+ CGI : /orders
Methods : POST
Argument : amount
Value: 0
Argument : clientName
```

11424 - WebDAV Detection -

Synopsis

The remote server is running with WebDAV enabled.

Description

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

If you do not use this extension, you should disable it.

Solution

http://support.microsoft.com/default.aspx?kbid=241520

Risk Factor

None

Plugin Information:

Published: 2003/03/20, Modified: 2011/03/14

Plugin Output

tcp/80