Report generated by Tenable Nessus™

DC-1

Fri, 20 Feb 2026 08:28:13 UTC

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

192.168.0.119

2	1	5	4	39
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Fri Feb 20 08:18:30 2026
End time:	Fri Feb 20 08:28:13 2026

Host Information

IP:	192.168.0.119
MAC Address:	08:00:27:95:D1:B6
OS:	Linux Kernel 3.2 on Debian 7.0 (wheezy)

Vulnerabilities

201366 - Debian Linux SEoL (7.x) -

Synopsis

An unsupported version of Debian Linux is installed on the remote host.

Description

According to its version, Debian Linux is 7.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

See Also

https://www.debian.org/News/2016/20160425

Solution

Upgrade to a version of Debian Linux 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 v2.0 Base Score

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

Plugin Information

Published: 2024/07/03, Modified: 2025/03/26

Plugin Output

tcp/22/ssh

```
OS : Debian Linux 7.0
Security End of Life : April 25, 2016
Time since Security End of Life (Est.) : >= 9 years
```

58987 - PHP Unsupported Version Detection -

Synopsis

The remote host contains an unsupported version of a web application scripting language.

Description

According to its version, the installation of PHP on the remote host is no longer supported.

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.

See Also

http://php.net/eol.php
https://wiki.php.net/rfc/releaseprocess

Solution

Upgrade to a version of PHP 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 v2.0 Base Score

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

References

XREF	IAVA:0001-A-0581

Plugin Information

Published: 2012/05/04, Modified: 2024/11/22

Plugin Output

tcp/80/www

```
Source : X-Powered-By: PHP/5.4.45-0+deb7u14
Installed version : 5.4.45-0+deb7u14
End of support date : 2015/09/03
Announcement : http://php.net/supported-versions.php
Supported versions : 8.1.x / 8.2.x / 8.3.x
```

78515 - Drupal Database Abstraction API SQLi -

Synopsis

The remote web server is running a PHP application that is affected by a SQL injection vulnerability.

Description

The remote web server is running a version of Drupal that is affected by a SQL injection vulnerability due to a flaw in the Drupal database abstraction API, which allows a remote attacker to use specially crafted requests that can result in arbitrary SQL execution. This may lead to privilege escalation, arbitrary PHP execution, or remote code execution.

See Also

https://www.drupal.org/SA-CORE-2014-005
https://www.drupal.org/project/drupal/releases/7.32

Solution

Upgrade to version 7.32 or later.

Risk Factor

High

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

6.2 (CVSS2#E:F/RL:OF/RC:C)

References

BID	70595
CVE	CVE-2014-3704
XREF	EDB-ID:34984
XREF	EDB-ID:34992
XREF	EDB-ID:34993
XREF	EDB-ID:35150

Exploitable With

CANVAS (true) Core Impact (true) (true) Metasploit (true)

Plugin Information

Published: 2014/10/16, Modified: 2022/04/11

Plugin Output

tcp/80/www

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

POST /?q=node&destination=node HTTP/1.1
Host: 192.168.0.119
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Content-Type: application/x-www-form-urlencoded
Connection: Keep-Alive
Content-Length: 117
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*

name[0;SELECT+@@version;#]=0;&name[0]=nessus&pass=nessus&test2=test&form_build_id=&form_id=user_login_block&op=Log+in


This produced the following truncated output (limited to 5 lines) :
------------------------------ snip ------------------------------
>Warning</em>: mb_strlen() expects parameter 1 to be string, array given in <em class="placeholder">drupal_strlen()</em> (line <em
class="placeholder">478</em> of <em class="placeholder">/var/www/includes/unicode.inc</em>).</li>
<li><em class="placeholder">Warning</em>: addcslashes() expects parameter 1 to be string, array given in <em
class="placeholder">DatabaseConnection-&gt;escapeLike()</em> (line <em class="placeholder">981</em> of <em
class="placeholder">/var/www/includes/database/database.inc</em>).</li>
<li>Sorry, unrecognized username or password. <a href="/user/password?
name[0%3BSELECT%20%40%40version%3B%23]=0%3B&amp;name[0]=nessus">Have you forgotten your password?</a></li>
</ul>
</div>
[...]
```

```
------------------------------ snip ------------------------------
```

136929 - JQuery 1.2 < 3.5.0 Multiple XSS -

Synopsis

The remote web server is affected by multiple cross site scripting vulnerability.

Description

According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities.

Note, the vulnerabilities referenced in this plugin have no security impact on PAN-OS, and/or the scenarios required for successful exploitation do not exist on devices running a PAN-OS release.

See Also

https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
https://security.paloaltonetworks.com/PAN-SA-2020-0007

Solution

Upgrade to JQuery version 3.5.0 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

5.7 (CVSS:3.0/E:F/RL:O/RC:C)

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

3.6 (CVSS2#E:F/RL:OF/RC:C)

STIG Severity

II

References

CVE	CVE-2020-11022
CVE	CVE-2020-11023
XREF	IAVB:2020-B-0030
XREF	CEA-ID:CEA-2021-0004
XREF	CEA-ID:CEA-2021-0025
XREF	CISA-KNOWN-EXPLOITED:2025/02/13

Plugin Information

Published: 2020/05/28, Modified: 2025/01/24

Plugin Output

tcp/80/www

```
URL : http://192.168.0.119/misc/jquery.js?v=1.4.4
Installed version : 1.4.4
Fixed version : 3.5.0
```

142591 - PHP < 7.3.24 Multiple Vulnerabilities -

Synopsis

The version of PHP running on the remote web server is affected by multiple vulnerabilities.

Description

According to its self-reported version number, the version of PHP running on the remote web server is prior to 7.3.24. It is, therefore affected by multiple vulnerabilities

See Also

https://www.php.net/ChangeLog-7.php#7.3.24

Solution

Upgrade to PHP version 7.3.24 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

STIG Severity

I

References

XREF	IAVA:2020-A-0510-S

Plugin Information

Published: 2020/11/06, Modified: 2025/05/26

Plugin Output

tcp/80/www

```
URL : http://192.168.0.119/ (5.4.45-0+deb7u14 under X-Powered-By: PHP/5.4.45-0+deb7u14)
Installed version : 5.4.45-0+deb7u14
Fixed version : 7.3.24
```

152853 - PHP < 7.3.28 Email Header Injection -

Synopsis

The version of PHP running on the remote web server is affected by an email header injection vulnerability.

Description

According to its self-reported version number, the version of PHP running on the remote web server is prior to 7.3.28.
It is, therefore affected by an email header injection vulnerability, due to a failure to properly handle CR-LF sequences in header fields. An unauthenticated, remote attacker can exploit this, by inserting line feed characters into email headers, to gain full control of email header content.

See Also

https://www.php.net/ChangeLog-7.php#7.3.28

Solution

Upgrade to PHP version 7.3.28 or later.

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 v2.0 Base Score

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

Plugin Information

Published: 2021/08/26, Modified: 2025/05/26

Plugin Output

tcp/80/www

```
URL : http://192.168.0.119/ (5.4.45-0+deb7u14 under X-Powered-By: PHP/5.4.45-0+deb7u14)
Installed version : 5.4.45-0+deb7u14
Fixed version : 7.3.28
```

90317 - SSH Weak Algorithms Supported -

Synopsis

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

Description

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

See Also

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

Solution

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

Risk Factor

Medium

CVSS v2.0 Base Score

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

Plugin Information

Published: 2016/04/04, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

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

arcfour
arcfour128
arcfour256

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

arcfour
arcfour128
arcfour256
```

121479 - web.config File Information Disclosure -

Synopsis

The remote web server hosts an application that is affected by an information disclosure vulnerability.

Description

An information disclosure vulnerability exists in the remote web server due to the disclosure of the web.config file. An unauthenticated, remote attacker can exploit this, via a simple GET request, to disclose potentially sensitive configuration information.

Solution

Ensure proper restrictions are in place, or remove the web.config file if the file 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 v2.0 Base Score

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

Plugin Information

Published: 2019/01/30, Modified: 2020/04/27

Plugin Output

tcp/80/www

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

GET /web.config HTTP/1.1
Host: 192.168.0.119
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*



This produced the following truncated output (limited to 5 lines) :
------------------------------ snip ------------------------------
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
<system.webServer>
<!-- Don't show directory listings for URLs which map to a directory. -->
<directoryBrowse enabled="false" />
[...]

------------------------------ snip ------------------------------
```

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

Low

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2024/10/07

Plugin Output

icmp/0

```
The difference between the local and remote clocks is -33154 seconds.
```

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 v3.0 Base Score

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

CVSS v2.0 Base Score

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

CVSS v2.0 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: 2023/10/27

Plugin Output

tcp/22/ssh

```

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

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

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

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

153953 - SSH Weak Key Exchange Algorithms Enabled -

Synopsis

The remote SSH server is configured to allow weak key exchange algorithms.

Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) RFC9142. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-sha1-*

rsa1024-sha1

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

See Also

https://datatracker.ietf.org/doc/html/rfc9142

Solution

Contact the vendor or consult product documentation to disable the weak algorithms.

Risk Factor

Low

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

Plugin Information

Published: 2021/10/13, Modified: 2024/03/22

Plugin Output

tcp/22/ssh

```
The following weak key exchange algorithms are enabled :

diffie-hellman-group-exchange-sha1
diffie-hellman-group1-sha1
```

71049 - SSH Weak MAC Algorithms Enabled -

Synopsis

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

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Solution

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

Risk Factor

Low

CVSS v2.0 Base Score

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

Plugin Information

Published: 2013/11/22, Modified: 2016/12/14

Plugin Output

tcp/22/ssh

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

hmac-md5
hmac-md5-96
hmac-sha1-96
hmac-sha2-256-96
hmac-sha2-512-96

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

hmac-md5
hmac-md5-96
hmac-sha1-96
hmac-sha2-256-96
hmac-sha2-512-96
```

18261 - Apache Banner Linux Distribution Disclosure -

Synopsis

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

Description

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

Solution

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

Risk Factor

None

Plugin Information

Published: 2005/05/15, Modified: 2025/03/31

Plugin Output

tcp/0

```
The Linux distribution detected was :
- Debian 7.0 (wheezy)
- Debian unstable (sid)
- Debian testing (wheezy)
```

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

References

XREF	IAVT:0001-T-0030
XREF	IAVT:0001-T-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/08/17

Plugin Output

tcp/80/www

```
URL : http://192.168.0.119/
Version : 2.2.99
Source : Server: Apache/2.2.22 (Debian)
backported : 1
os : ConvertedDebian
```

39520 - Backported Security Patch Detection (SSH) -

Synopsis

Security patches are backported.

Description

Security patches may have been 'backported' to the remote SSH server without changing its version number.

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

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

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/22/ssh

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

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/www

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

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: 2025/07/14

Plugin Output

tcp/0

```
Following application CPE's matched on the remote system :

cpe:/a:apache:http_server:2.2.22 -> Apache Software Foundation Apache HTTP Server
cpe:/a:apache:http_server:2.2.99 -> Apache Software Foundation Apache HTTP Server
cpe:/a:drupal:drupal:7 -> Drupal
cpe:/a:jquery:jquery:1.4.4 -> jQuery
cpe:/a:openbsd:openssh:6.0 -> OpenBSD OpenSSH
cpe:/a:openbsd:openssh:6.0p1 -> OpenBSD OpenSSH
cpe:/a:php:php:5.4.45 -> PHP PHP
cpe:/a:php:php:5.4.45-0%2bdeb7u14 -> PHP PHP
```

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: 2025/03/12

Plugin Output

tcp/0

```
Remote device type : general-purpose
Confidence level : 95
```

18638 - Drupal Software Detection -

Synopsis

A content management system is running on the remote web server.

Description

Drupal, an open source content management system written in PHP, is running on the remote web server.

See Also

https://www.drupal.org/

Solution

Ensure that the use of this software aligns with your organization's security and acceptable use policies.

Risk Factor

None

References

XREF	IAVT:0001-T-0586

Plugin Information

Published: 2005/07/07, Modified: 2023/05/24

Plugin Output

tcp/80/www

```
URL : http://192.168.0.119/
Version : 7
```

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: 2020/05/13

Plugin Output

tcp/0

```
The following card manufacturers were identified :
```

```
08:00:27:95:D1:B6 : 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: 2025/06/10

Plugin Output

tcp/0

```
The following is a consolidated list of detected MAC addresses:
- 08:00:27:95:D1:B6
```

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

References

XREF	IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :

Apache/2.2.22 (Debian)
```

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 is 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: 2024/02/26

Plugin Output

tcp/80/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

Date: Wed, 18 Feb 2026 17:35:58 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.45-0+deb7u14
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Last-Modified: Wed, 18 Feb 2026 17:35:58 +0000
Cache-Control: no-cache, must-revalidate, post-check=0, pre-check=0
ETag: "1771436158"
Content-Language: en
X-Generator: Drupal 7 (http://drupal.org)
Vary: Accept-Encoding
Content-Length: 7606
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8

Response Body :

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML+RDFa 1.0//EN"
"http://www.w3.org/MarkUp/DTD/xhtml-rdfa-1.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" version="XHTML+RDFa 1.0" dir="ltr"
xmlns:content="http://purl.org/rss/1.0/modules/content/"
xmlns:dc="http://purl.org/dc/terms/"
xmlns:foaf="http://xmlns.com/foaf/0.1/"
xmlns:og="http://ogp.me/ns#"
xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
xmlns:sioc="http://rdfs.org/sioc/ns#"
xmlns:sioct="http://rdfs.org/sioc/types#"
xmlns:skos="http://www.w3.org/2004/02/skos/core#"
xmlns:xsd="http://www.w3.org/2001/XMLSchema#">

<head profile="http://www.w3.org/1999/xhtml/vocab">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link rel="shortcut icon" href="http://192.168.0.119/misc/favicon.ico" type="image/vnd.microsoft.icon" />
<meta name="Generator" content="Drupal 7 (http://drupal.org)" />
<title>Welcome to Drupal Site | Drupal Site</title>
<style type="text/css" media="all">@import url("http://192.168.0.119/modules/system/system.base.css?pn6csl");
@import url("http://192.168.0.119/modules/system/system.menus.css?pn6csl");
@import url("http://192.168.0.119/modules/system/system.messages.css?pn6csl");
@import url("http://192.168.0.119/modules/system/system.theme.css?pn6csl");</style>
<style type="text/css" media="all">@import url("http://192.168.0.119/modules/field/theme/field.css?pn6csl");
@import url("http://192.168.0.119/modules/node/node.css?pn6csl");
@import url("http://192.168.0.119/modules/search/search.css?pn6csl");
@import url("http://192.168.0.119/modules/user/user.css?pn6csl");
@import url("http://192.168.0.119/sites/all/modules/views/css/views.css?pn6csl");</style>
<style type="text/css" media="all">@import url("http://192.168.0.119/sites/all/modules/ctools/css/ctools.css?pn6csl");</style>
<style type="text/css" media="all">@import url("http://192.168.0.119/themes/bartik/css/layout.css?pn6csl");
@import url("http://192.168.0.119/themes/bartik/css/style.css?pn6csl");
@import url("http://192.168.0.119/themes/bartik/css/colors.css?pn6csl");</style>
<style type="text/css" media="print">@import url("http://192.168.0.119/themes/bartik/css/print.css?pn6csl");</style>

<!--[if lte IE 7]>
<link type="text/css" rel="stylesheet" href="http://192.168.0.119/themes/bartik/css/ie.css?pn6csl" media="all" />
<![endif]-->

<!--[if IE 6]>
<link type="text/css" rel="stylesheet" href="http://192.168.0.119/themes/bartik/css/ie6.css?pn6csl" media="all" />
<![endif]-->
<script type="text/javascript" src="http://192.168.0.119/misc/jquery.js?v=1.4.4"></script>
<script type="text/javascript" src="http://192.168.0.119/misc/jquery.once.js?v=1.2"></script>
<script type="text/javascript" src="http://192.168.0.119/misc/drupal.js?pn6csl"></script>
<script type="text/javascript">
<!--//--><![CDATA[//><!--
jQuery.extend(Drupal.settings, {"basePath":"\/","pathPrefix":"","ajaxPageState":
{"theme":"bartik","theme_token":"0Wgzu2mqTb3ZG7bd8E4eHiK4SCG6RlOQD_0sQ4BG9A8","js":
```

```
{"misc\/jquery.js":1,"misc\/jquery.once.js":1,"misc\/drupal.js":1},"css":
{"modules\/system\/system.base.css":1,"modules\/system\/system.menus.css":1,"modules\/system\/system.messages.css":1,"modules\/syste
m\/system.theme.css":1,"modules\/field\/theme\/field.css":1,"modules\/node\/node.css":1,"modules\/search\/search.css":1,"modules\/us
er\/user.css":1,"sites\/all\/modules\/views\/css\/views.css":1,"sites\/all\/modules\/ctools\/css\/ctools.css":1,"themes\/bartik\/css
\/layout.css":1,"themes\/bartik\/css\/style.css":1,"themes\/bartik\/css\/colors.css":1,"themes\/bartik\/css\/print.css":1,"themes\/b
artik\/css\/ie.css":1,"themes\/bartik\/css\/ie6.css":1}}});
//--><!]]>
</script>
</head>
<body class="html front not-logged-in one-sidebar sidebar-first page-node" >
<div id="skip-link">
<a href="#main-content" class="element-invisible element-focusable">Skip to main content</a>
</div>
<div id="page-wrapper"><div id="page">

<div id="header" class="without-secondary-menu"><div class="section clearfix">

<a href="/" title="Home" rel="home" id="logo">
<img src="http://192.168.0.119/themes/bartik/logo.png" alt="Home" />
</a>

<div id="name-and-slogan">

<div id="site-name">
<strong>
<a href="/" title="Home" rel="home"><span>Drupal Site</span></a>
</strong>
</div>


</div> <!-- /#name-and-slogan -->


<div id="main-menu" class="navigation">
<h2 class="element-invisible">Main menu</h2><ul id="main-menu-links" class="links clearfix"><li class="menu-218 first last active">
<a href="/" class="active">Home</a></li>
</ul> </div> <!-- /#main-menu -->


</div></div> <!-- /.section, /#header -->



<div id="main-wrapper" class="clearfix"><div id="main" class="clearfix">


<div id="sidebar-first" class="column sidebar"><div class="section">
<div class="region region-sidebar-first">
<div id="block-user-login" class="block block-user">

<h2>User login</h2>

<div class="content">
<form action="/node?destination=node" method="post" id="user-login-form" accept-charset="UTF-8"><div><div class="form-item form-
type-textfield form-item-name">
<label for="edit-name">Username <span class="form-required" title="This field is required.">*</span></label>
<input type="text" id="edit-name" name="name" value="" size="15" maxlength="60" class="form-text required" />
</div>
<div class="form-item form-type-password form-item-pass">
<label for="edit-pass">Password <span class="form-required" title="This field is required.">*</span></label>
<input type="password" id="edit-pass" name="pass" size="15" maxlength="128" class="form-text required" />
</div>
<div class="item-list"><ul><li class="first"><a href="/user/register" title="Create a new user account.">Create new account</a></li>
<li class="last"><a href="/user/password" title="Request new password via e-mail.">Request new password</a></li>
</ul></div><input type="hidden" name="form_build_id" value="form-NxjuCVg5--UTrZhl14oZTU5RX3eElcH5iLNnsxRBWwc" />
<input type="hidden" name="form_id" value="user_login_block" />
<div class="form-actions form-wrapper" id="edit-actions"><input type="submit" id="edit-submit" name="op" value="Log in" class="form-
submit" /></div></div></form> </div>
</div>
</div>
</div></div> <!-- /.section, /#sidebar-first -->

<div id="content" class="column"><div class="section">
<a id="main-content"></a>
<h1 class="title" id="page-title">
Welcome to Drupal Site </h1>
<div class="tabs">
</div>
<div class="region region-content">
<div id="block-system-main" class="block block-system">


<div class="content">
<div id="first-time"><p>No front page content has been created yet.</p></div> </div>
</div>
</div>

</div></div> <!-- /.section, /#content -->


</div></div> <!-- /#main, /#main-wrapper -->


<div id="footer-wrapper"><div class="section">


<div id="footer" class="clearfix">
<div class="region region-footer">
<div id="block-system-powered-by" class="block block-system">
```

```
<div class="content">
<span>Powered by <a href="http://drupal.org">Drupal</a></span> </div>
</div>
</div>
</div> <!-- /#footer -->

</div></div> <!-- /.section, /#footer-wrapper -->

</div></div> <!-- /#page, /#page-wrapper -->
</body>
</html>
```

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: 2024/02/08

Plugin Output

tcp/80/www

```
URL : http://192.168.0.119/misc/jquery.js?v=1.4.4
Version : 1.4.4
```

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: 2025/07/14

Plugin Output

tcp/22/ssh

```
Port 22/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: 2025/07/14

Plugin Output

tcp/80/www

```
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: 2025/07/14

Plugin Output

tcp/111/rpc-portmapper

```
Port 111/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.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- 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: 2025/06/25

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.9.3
Nessus build : 20023
Plugin feed version : 202508200628
Scanner edition used : Nessus

ERROR: Your plugins have not been updated since 2025/8/20
Performing a scan with an older plugin set will yield out-of-date results and
produce an incomplete audit. Please run nessus-update-plugins to get the
newest vulnerability checks from Nessus.org.

Scanner OS : LINUX
Scanner distribution : ubuntu1604-x86-64
Scan type : Normal
Scan name : DC-1
Scan policy used : Advanced Scan
Scanner IP : 192.168.0.108
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 120.413 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 100
Max checks : 5
Recv timeout : 5
Backports : Detected
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2026/2/20 8:18 UTC
Scan duration : 579 sec
Scan for malware : no
```

209654 - OS Fingerprints Detected -

Synopsis

Multiple OS fingerprints were detected.

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, “OS Identification”, the complete set of fingerprints detected are reported here.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/02/26, Modified: 2025/03/03

Plugin Output

tcp/0

```
Following OS Fingerprints were found

Remote operating system : Debian 7.0 Linux Kernel 3.2
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : Linux Kernel 3.2 on Debian 7.0 (wheezy)
Confidence level : 95
Method : SSH
Type : general-purpose
Fingerprint : SSH:SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u7

Remote operating system : Linux Kernel 3.2 on Debian 7.0 (wheezy)
Debian unstable (sid)
Debian testing (wheezy)
Confidence level : 45
Method : HTTP
Type : general-purpose
Fingerprint : unknown

Remote operating system : Linux Kernel 2.x
Confidence level : 54
Method : SinFP
Type : general-purpose
Fingerprint : SinFP:
P1:B10113:F0x12:W14600:O0204ffff:M1460:
P2:B10113:F0x12:W14480:O0204ffff0402080affffffff4445414401030304:M1460:
P3:B00000:F0x00:W0:O0:M0
P4:191303_7_p=22
```

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: 2025/06/03

Plugin Output

tcp/0

```
Remote operating system : Linux Kernel 3.2 on Debian 7.0 (wheezy)
Confidence level : 95
Method : SSH


The remote host is running Linux Kernel 3.2 on Debian 7.0 (wheezy)
```

117886 - OS Security Patch Assessment Not Available -

Synopsis

OS Security Patch Assessment is not available.

Description

OS Security Patch Assessment is not available on the remote host.
This does not necessarily indicate a problem with the scan.
Credentials may not have been provided, OS security patch assessment may not be supported for the target, the target may not have been identified, or another issue may have occurred that prevented OS security patch assessment from being available. See plugin output for details.

This plugin reports non-failure information impacting the availability of OS Security Patch Assessment. Failure information is reported by plugin 21745 : 'OS Security Patch Assessment failed'. If a target host is not supported for OS Security Patch Assessment, plugin 110695 : 'OS Security Patch Assessment Checks Not Supported' will report concurrently with this plugin.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0515

Plugin Information

Published: 2018/10/02, Modified: 2021/07/12

Plugin Output

tcp/0

```
The following issues were reported :

- Plugin : no_local_checks_credentials.nasl
Plugin ID : 110723
Plugin Name : Target Credential Status by Authentication Protocol - No Credentials Provided
Message :
Credentials were not provided for detected SSH service.
```

181418 - OpenSSH Detection -

Synopsis

An OpenSSH-based SSH server was detected on the remote host.

Description

An OpenSSH-based SSH server was detected on the remote host.

See Also

https://www.openssh.com/

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2023/09/14, Modified: 2025/08/19

Plugin Output

tcp/22/ssh

```
Service : ssh
Version : 6.0p1
Banner : SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u7
```

48243 - PHP Version Detection -

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0936

Plugin Information

Published: 2010/08/04, Modified: 2025/05/26

Plugin Output

tcp/80/www

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

Version : 5.4.45-0+deb7u14
Source : X-Powered-By: PHP/5.4.45-0+deb7u14
```

66334 - Patch Report -

Synopsis

The remote host is missing several patches.

Description

The remote host is missing one or more security patches. This plugin lists the newest version of each patch to install to make sure the remote host is up-to-date.

Note: Because the 'Show missing patches that have been superseded' setting in your scan policy depends on this plugin, it will always run and cannot be disabled.

Solution

Install the patches listed below.

Risk Factor

None

Plugin Information

Published: 2013/07/08, Modified: 2025/08/12

Plugin Output

tcp/0

```
. You need to take the following action :

[ JQuery 1.2 < 3.5.0 Multiple XSS (136929) ]

+ Action to take : Upgrade to JQuery version 3.5.0 or later.
```

11111 - RPC Services Enumeration -

Synopsis

An ONC RPC service is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/111/rpc-portmapper

```
The following RPC services are available on TCP port 111 :

- program: 100000 (portmapper), version: 4
- program: 100000 (portmapper), version: 3
- program: 100000 (portmapper), version: 2
```

11111 - RPC Services Enumeration -

Synopsis

An ONC RPC service is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/111/rpc-portmapper

```
The following RPC services are available on UDP port 111 :

- program: 100000 (portmapper), version: 4
- program: 100000 (portmapper), version: 3
- program: 100000 (portmapper), version: 2
```

11111 - RPC Services Enumeration -

Synopsis

An ONC RPC service is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

udp/39804/rpc-status

```
The following RPC services are available on UDP port 39804 :

- program: 100024 (status), version: 1
```

11111 - RPC Services Enumeration -

Synopsis

An ONC RPC service is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/08/24, Modified: 2011/05/24

Plugin Output

tcp/55946/rpc-status

```
The following RPC services are available on TCP port 55946 :

- program: 100024 (status), version: 1
```

53335 - RPC portmapper (TCP) -

Synopsis

An ONC RPC portmapper is running on the remote host.

Description

The RPC portmapper is running on this port.

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/04/08, Modified: 2011/08/29

Plugin Output

tcp/111/rpc-portmapper

10223 - RPC portmapper Service Detection -

Synopsis

An ONC RPC portmapper is running on the remote host.

Description

The RPC portmapper is running on this port.

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

Solution

n/a

Risk Factor

None

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0632

Plugin Information

Published: 1999/08/19, Modified: 2019/10/04

Plugin Output

udp/111/rpc-portmapper

70657 - SSH Algorithms and Languages Supported -

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/10/28, Modified: 2025/01/20

Plugin Output

tcp/22/ssh

```
Nessus negotiated the following encryption algorithm(s) with the server :

Client to Server: aes256-ctr
Server to Client: aes256-ctr

The server supports the following options for compression_algorithms_server_to_client :

none
zlib@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-ripemd160@openssh.com
hmac-sha1
hmac-sha1-96
hmac-sha2-256
```

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

  The server supports the following options for server_host_key_algorithms :

  ecdsa-sha2-nistp256
  ssh-dss
  ssh-rsa

  The server supports the following options for encryption_algorithms_client_to_server :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

  The server supports the following options for mac_algorithms_server_to_client :

  hmac-md5
  hmac-md5-96
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1
  hmac-sha1-96
  hmac-sha2-256
  hmac-sha2-256-96
  hmac-sha2-512
  hmac-sha2-512-96
  umac-64@openssh.com

  The server supports the following options for kex_algorithms :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group1-sha1
  diffie-hellman-group14-sha1
  ecdh-sha2-nistp256
  ecdh-sha2-nistp384
  ecdh-sha2-nistp521

  The server supports the following options for compression_algorithms_client_to_server :

  none
  zlib@openssh.com

  The server supports the following options for encryption_algorithms_server_to_client :

  3des-cbc
  aes128-cbc
  aes128-ctr
  aes192-cbc
  aes192-ctr
  aes256-cbc
  aes256-ctr
  arcfour
  arcfour128
  arcfour256
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
```

149334 - SSH Password Authentication Accepted -

Synopsis

The SSH server on the remote host accepts password authentication.

Description

The SSH server on the remote host accepts password authentication.

See Also

https://tools.ietf.org/html/rfc4252#section-8

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/05/07, Modified: 2021/05/07

Plugin Output

tcp/22/ssh

10881 - SSH Protocol Versions Supported -

Synopsis

A SSH server is running on the remote host.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/03/06, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

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

- 1.99
- 2.0
```

153588 - SSH SHA-1 HMAC Algorithms Enabled -

Synopsis

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Description

The remote SSH server is configured to enable SHA-1 HMAC algorithms.

Although NIST has formally deprecated use of SHA-1 for digital signatures, SHA-1 is still considered secure for HMAC as the security of HMAC does not rely on the underlying hash function being resistant to collisions.

Note that this plugin only checks for the options of the remote SSH server.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2021/09/23, Modified: 2022/04/05

Plugin Output

tcp/22/ssh

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :

hmac-sha1
hmac-sha1-96

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :
hmac-sha1
hmac-sha1-96
```

10267 - SSH Server Type and Version Information -

Synopsis

An SSH server is listening on this port.

Description

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

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0933

Plugin Information

Published: 1999/10/12, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

```
  SSH version : SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u7
  SSH supported authentication : publickey,password
```

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: 2024/03/26

Plugin Output

tcp/22/ssh

```
  An SSH 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: 2024/03/26

Plugin Output

tcp/80/www

```
  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: 2023/10/17

Plugin Output

tcp/0

110723 - Target Credential Status by Authentication Protocol - No Credentials Provided -

Synopsis

Nessus was able to find common ports used for local checks, however, no credentials were provided in the scan policy.

Description

Nessus was not able to successfully authenticate directly to the remote target on an available authentication protocol. Nessus was able to connect to the remote port and identify that the service running on the port supports an authentication protocol, but Nessus failed to authenticate to the remote service using the provided credentials. There may have been a protocol failure that prevented authentication from being attempted or all of the provided credentials for the authentication protocol may be invalid. See plugin output for error details.

Please note the following :

- This plugin reports per protocol, so it is possible for valid credentials to be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- Providing valid credentials for all available authentication protocols may improve scan coverage, but the value of successful authentication for a given protocol may vary from target to target depending upon what data (if any) is gathered from the target via that protocol. For example, successful authentication via SSH is more valuable for Linux targets than for Windows targets, and likewise successful authentication via SMB is more valuable for Windows targets than for Linux targets.

Solution

n/a

Risk Factor

None

References

XREF	IAVB:0001-B-0504

Plugin Information

Published: 2018/06/27, Modified: 2024/04/19

Plugin Output

tcp/0

```
SSH was detected on port 22 but no credentials were provided.
SSH local checks were not enabled.
```

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: 2023/12/04

Plugin Output

udp/0

```
For your information, here is the traceroute from 192.168.0.108 to 192.168.0.119 :
192.168.0.108
192.168.0.119

Hop Count: 1
```

10302 - Web Server robots.txt Information Disclosure -

Synopsis

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

Description

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

See Also

http://www.robotstxt.org/orig.html

Solution

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

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2018/11/15

Plugin Output

tcp/80/www

```
Contents of robots.txt :

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

User-agent: *
Crawl-delay: 10
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /INSTALL.sqlite.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
Disallow: /user/logout/
# Paths (no clean URLs)
Disallow: /?q=admin/
Disallow: /?q=comment/reply/
Disallow: /?q=filter/tips/
Disallow: /?q=node/add/
Disallow: /?q=search/
Disallow: /?q=user/password/
Disallow: /?q=user/register/
Disallow: /?q=user/login/
Disallow: /?q=user/logout/
```

Compliance 'FAILED'

Compliance 'SKIPPED'

Compliance 'PASSED'

Compliance 'INFO', 'WARNING', 'ERROR'

Remediations

Suggested Remediations