Basic Scan

Report generated by Nessus™ Sat, 03 Jun 2023 10:36:26 CEST

TABLE OF CONTENTS

Vulnerabilities by Plugin

Vulnerabilities by Plugin

150280 (1) - Apache 2.4.x < 2.4.47 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.47. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.47 changelog:

- Unexpected <Location> section matching with 'MergeSlashes OFF' (CVE-2021-30641)

- mod_auth_digest: possible stack overflow by one nul byte while validating the Digest nonce. (CVE-2020-35452)

- mod_session: Fix possible crash due to NULL pointer dereference, which could be used to cause a Denial of Service with a malicious backend server and SessionHeader. (CVE-2021-26691)

- mod_session: Fix possible crash due to NULL pointer dereference, which could be used to cause a Denial of Service.

(CVE-2021-26690)

- mod_proxy_http: Fix possible crash due to NULL pointer dereference, which could be used to cause a Denial of Service. (CVE-2020-13950)

- Windows: Prevent local users from stopping the httpd process (CVE-2020-13938)

- mod_proxy_wstunnel, mod_proxy_http: Handle Upgradable protocols end-to-end negotiation. (CVE-2019-17567)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://downloads.apache.org/httpd/CHANGES_2.4

Solution

Upgrade to Apache version 2.4.47 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

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

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

STIG Severity

I

References

CVE	CVE-2019-17567
CVE	CVE-2020-13938
CVE	CVE-2020-13950
CVE	CVE-2020-35452
CVE	CVE-2021-26690
CVE	CVE-2021-26691
CVE	CVE-2021-30641
XREF	IAVA:2021-A-0259-S

Plugin Information

Published: 2021/06/04, Modified: 2022/04/11

Plugin Output

192.168.64.7 (tcp/80/www)

```
URL              : http://192.168.64.7/
Installed version : 2.4.46
Fixed version     : 2.4.47
```

153583 (1) - Apache < 2.4.49 Multiple Vulnerabilities

Synopsis

The remote web server is affected by a vulnerability.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.49. It is, therefore, affected by a vulnerability as referenced in the 2.4.49 changelog.

- A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. (CVE-2021-40438)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://downloads.apache.org/httpd/CHANGES_2.4

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.49 or later.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.1

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-40438
XREF	IAVA:2021-A-0440-S
XREF	CISA-KNOWN-EXPLOITED:2021/12/15

Plugin Information

Published: 2021/09/23, Modified: 2023/04/25

Plugin Output

192.168.64.7 (tcp/80/www)

```
URL               : http://192.168.64.7/
Installed version : 2.4.46
Fixed version     : 2.4.49
```

153584 (1) - Apache < 2.4.49 Multiple Vulnerabilities

Synopsis

The remote web server is affected by a vulnerability.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.49. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.49 changelog.

- ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. (CVE-2021-39275)

- Malformed requests may cause the server to dereference a NULL pointer. (CVE-2021-34798)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://downloads.apache.org/httpd/CHANGES_2.4

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.49 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

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

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

STIG Severity

I

References

CVE	CVE-2021-34798
CVE	CVE-2021-39275
XREF	IAVA:2021-A-0440-S

Plugin Information

Published: 2021/09/23, Modified: 2022/04/11

Plugin Output

192.168.64.7 (tcp/80/www)

```
URL               : http://192.168.64.7/
Installed version : 2.4.46
Fixed version     : 2.4.49
```

156255 (1) - Apache 2.4.x >= 2.4.7 / < 2.4.52 Forward Proxy DoS / SSRF

Synopsis

The remote web server is affected by a denial of service or server-side request forgery vulnerability.

Description

The version of Apache httpd installed on the remote host is equal to or greater than 2.4.7 and prior to 2.4.52.

It is, therefore, affected by a flaw related to acting as a forward proxy.

A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery).

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.52 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.4

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

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

STIG Severity

I

References

CVE	CVE-2021-44224
CVE	CVE-2021-44790
XREF	IAVA:2021-A-0604-S

Plugin Information

Published: 2021/12/23, Modified: 2023/04/03

Plugin Output

192.168.64.7 (tcp/80/www)

```
URL               : http://192.168.64.7/
Installed version : 2.4.46
Fixed version     : 2.4.52
```

158900 (1) - Apache 2.4.x < 2.4.53 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.53. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.53 advisory.

- mod_lua Use of uninitialized value of in r:parsebody: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Chamal De Silva (CVE-2022-22719)

- HTTP request smuggling: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling Acknowledgements: James Kettle <james.kettle portswigger.net> (CVE-2022-22720)

- Possible buffer overflow with very large or unlimited LimitXMLRequestBody in core: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Anonymous working with Trend Micro Zero Day Initiative (CVE-2022-22721)

- Read/write beyond bounds in mod_sed: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions. Acknowledgements: Ronald Crane (Zippenhop LLC) (CVE-2022-23943)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

http://www.apache.org/dist/httpd/Announcement2.4.html

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.53 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

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

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

STIG Severity

I

References

CVE	CVE-2022-22719
CVE	CVE-2022-22720
CVE	CVE-2022-22721
CVE	CVE-2022-23943
XREF	IAVA:2022-A-0124-S

Plugin Information

Published: 2022/03/14, Modified: 2022/06/15

Plugin Output

192.168.64.7 (tcp/80/www)

```
URL               : http://192.168.64.7/
Installed version : 2.4.46
Fixed version     : 2.4.53
```

161454 (1) - Apache 2.4.x < 2.4.52 mod_lua Buffer Overflow

Synopsis

The remote web server is affected by a buffer overflow vulnerability.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.52. It is, therefore, affected by a flaw related to mod_lua when handling multipart content. A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerability though it might be possible to craft one.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.52 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

8.4

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

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

STIG Severity

I

References

CVE	CVE-2021-44790
XREF	IAVA:2021-A-0604-S

Plugin Information

Published: 2022/05/24, Modified: 2023/04/03

Plugin Output

192.168.64.7 (tcp/80/www)

```
URL               : http://192.168.64.7/
Installed version : 2.4.46
Fixed version     : 2.4.52
```

161948 (1) - Apache 2.4.x < 2.4.54 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.54. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.54 advisory.

- Possible request smuggling in mod_proxy_ajp: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions. Acknowledgements: Ricter Z @ 360 Noah Lab (CVE-2022-26377)

- Read beyond bounds in mod_isapi: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28330)

- Read beyond bounds via ap_rwrite(): The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28614)

- Read beyond bounds in ap_strcmp_match(): Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28615)

- Denial of service in mod_lua r:parsebody: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-29404)

- Denial of Service mod_sed: If Apache HTTP Server 2.4.53 is configured to do transformations with mod_sed in contexts where the input to mod_sed may be very large, mod_sed may make excessively large memory allocations and trigger an abort. Acknowledgements: This issue was found by Brian Moussalli from the JFrog Security Research team (CVE-2022-30522)

- Information Disclosure in mod_lua with websockets: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-30556)

- X-Forwarded-For dropped by hop-by-hop mechanism in mod_proxy: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/ application.

Acknowledgements: The Apache HTTP Server project would like to thank Gaetan Ferry (Synacktiv) for reporting this issue (CVE-2022-31813)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

See Also

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.54 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.4

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

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

STIG Severity

I

References

CVE	CVE-2022-26377
CVE	CVE-2022-28330
CVE	CVE-2022-28614
CVE	CVE-2022-28615
CVE	CVE-2022-29404

CVE	CVE-2022-30522
CVE	CVE-2022-30556
CVE	CVE-2022-31813
XREF	IAVA:2022-A-0230-S

Plugin Information

Published: 2022/06/08, Modified: 2023/01/19

Plugin Output

192.168.64.7 (tcp/80/www)

```
URL              : http://192.168.64.7/
Installed version : 2.4.46
Fixed version     : 2.4.54
```

170113 (1) - Apache 2.4.x < 2.4.55 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.55. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.55 advisory.

- A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash. This issue affects Apache HTTP Server 2.4.54 and earlier. (CVE-2006-20001)

- Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

(CVE-2022-36760)

- Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client. (CVE-2022-37436)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.55 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

7.3

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2006-20001
CVE	CVE-2022-36760
CVE	CVE-2022-37436
XREF	IAVA:2023-A-0047-S

Plugin Information

Published: 2023/01/18, Modified: 2023/03/10

Plugin Output

192.168.64.7 (tcp/80/www)

```
URL               : http://192.168.64.7/
Installed version : 2.4.46
Fixed version     : 2.4.55
```

172186 (1) - Apache 2.4.x < 2.4.56 Multiple Vulnerabilities

Synopsis

The remote web server is affected by multiple vulnerabilities.

Description

The version of Apache httpd installed on the remote host is prior to 2.4.56. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.56 advisory.

- HTTP request splitting with mod_rewrite and mod_proxy: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule ^/here/(.*) http://example.com:8080/elsewhere?$1 http://example.com:8080/elsewhere ; [P] ProxyPassReverse /here/ http://example.com:8080/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Acknowledgements: finder: Lars Krapf of Adobe (CVE-2023-25690)

- Apache HTTP Server: mod_proxy_uwsgi HTTP response splitting: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55.

Special characters in the origin response header can truncate/split the response forwarded to the client.

Acknowledgements: finder: Dimas Fariski Setyawan Putra (nyxsorcerer) (CVE-2023-27522)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.56 or later.

Risk Factor

Critical

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

9.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2023-25690
CVE	CVE-2023-27522
XREF	IAVA:2023-A-0124

Plugin Information

Published: 2023/03/07, Modified: 2023/03/15

Plugin Output

192.168.64.7 (tcp/80/www)

```
URL               : http://192.168.64.7/
Installed version : 2.4.46
Fixed version     : 2.4.56
```

153585 (1) - Apache >= 2.4.17 < 2.4.49 mod_http2

Synopsis

The remote web server is affected by a vulnerability.

Description

The version of Apache httpd installed on the remote host is greater than 2.4.17 and prior to 2.4.49. It is, therefore, affected by a vulnerability as referenced in the 2.4.49 changelog. A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://downloads.apache.org/httpd/CHANGES_2.4

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.49 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:H/A:N)

CVSS v3.0 Temporal Score

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

VPR Score

4.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-33193
XREF	IAVA:2021-A-0440-S

Plugin Information

Published: 2021/09/23, Modified: 2022/04/11

Plugin Output

192.168.64.7 (tcp/80/www)

```
URL               : http://192.168.64.7/
Installed version : 2.4.46
Fixed version     : 2.4.49
```

153586 (1) - Apache >= 2.4.30 < 2.4.49 mod_proxy_uwsgi

Synopsis

The remote web server is affected by a vulnerability.

Description

The version of Apache httpd installed on the remote host greater than 2.4.30 and is prior to 2.4.49. It is, therefore, affected by a vulnerability as referenced in the 2.4.49 changelog. A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS).

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

See Also

https://downloads.apache.org/httpd/CHANGES_2.4

https://httpd.apache.org/security/vulnerabilities_24.html

Solution

Upgrade to Apache version 2.4.49 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 v3.0 Temporal Score

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

VPR Score

4.4

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

CVE	CVE-2021-36160
XREF	IAVA:2021-A-0440-S

Plugin Information

Published: 2021/09/23, Modified: 2022/04/11

Plugin Output

192.168.64.7 (tcp/80/www)

```
URL               : http://192.168.64.7/
Installed version : 2.4.46
Fixed version     : 2.4.49
```

10107 (1) - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

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

Plugin Output

192.168.64.7 (tcp/80/www)

```
The remote web server type is :

Apache/2.4.46 (Debian)
```

10114 (1) - 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

CVSS v3.0 Base Score

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

CVSS v2.0 Base Score

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

References

CVE	CVE-1999-0524
XREF	CWE:200

Plugin Information

Published: 1999/08/01, Modified: 2023/04/27

Plugin Output

192.168.64.7 (icmp/0)

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

10287 (1) - Traceroute Information

Synopsis

It was possible to obtain traceroute information.

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/05/03

Plugin Output

192.168.64.7 (udp/0)

```
For your information, here is the traceroute from 192.168.64.6 to 192.168.64.7 :
192.168.64.6
192.168.64.7

Hop Count: 1
```

11219 (1) - 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: 2023/05/31

Plugin Output

192.168.64.7 (tcp/80/www)

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

11936 (1) - 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: 2022/03/09

Plugin Output

192.168.64.7 (tcp/0)

```
Remote operating system : Linux Kernel 2.6
Confidence level : 65
Method : SinFP


The remote host is running Linux Kernel 2.6
```

19506 (1) - 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: 2023/04/27

Plugin Output

192.168.64.7 (tcp/0)

```
Information about this scan :

Nessus version : 10.5.2
Nessus build : 20009
Plugin feed version : 202306030200
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : ubuntu1804-aarch64
Scan type : Normal
```

```
Scan name : Basic Scan
Scan policy used : Basic Network Scan
Scanner IP : 192.168.64.6
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 202.760 ms
Thorough tests : no
Experimental tests : 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 launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Scan Start Date : 2023/6/3 10:29 CEST
Scan duration : 431 sec
Scan for malware : no
```

22964 (1) - 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: 2023/03/29

Plugin Output

192.168.64.7 (tcp/80/www)

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

24260 (1) - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

192.168.64.7 (tcp/80/www)

```
Response Code : HTTP/1.1 200 OK

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

  Date: Sat, 03 Jun 2023 08:30:32 GMT
  Server: Apache/2.4.46 (Debian)
  Last-Modified: Sat, 30 Oct 2021 05:01:19 GMT
  ETag: "654-5cf8ad59e198a"
  Accept-Ranges: bytes
  Content-Length: 1620
  Vary: Accept-Encoding
  Keep-Alive: timeout=5, max=100
  Connection: Keep-Alive
  Content-Type: text/html

Response Body :

<!DOCTYPE html>
<html>

<head>
    <title></title>
```

```
</head>
<script type="text/javascript" src="javascript.js"></script>
<link rel="stylesheet" href="bootstrap.min.css">

<body>
    <nav class="navbar navbar-inverse navbar-fixed-top" role="navigation">
        <div class="container">
            <!-- Brand and toggle get grouped for better mobile display -->
            <div class="navbar-header">
                <button type="button" class="navbar-toggle" data-toggle="collapse" data-target="#bs-
example-navbar-collapse-1">
                    <span class="sr-only">Toggle navigation</span>
                    <span class="icon-bar"></span>
                    <span class="icon-bar"></span>
                    <span class="icon-bar"></span>
                </button>
                <a class="navbar-brand" href="#">
                    <font size="40" color="white">&#9763;</font>
                </a>
            </div>
            <!-- Collect the nav links, forms, and other content for toggling -->
            <div class="collapse navbar-collapse" id="bs-example-navbar-collapse-1">
                <ul class="nav navbar-nav">
                    <li>
                        <a href="#">about us</a>
                    </li>
                    <li>
                        <a href="profile.php">profile</a>
                    </li>
                </ul>
            </div>
            <!-- /.navbar-collapse -->
        </div>
        <!-- /.container -->
    </nav>
    <br><br><br><br>
    <center>
        <h1> WELCOME IN BLOG</h1>
        <h3>this is first blog</h3>
    < [...]
```

25220 (1) - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

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

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

192.168.64.7 (tcp/0)

43111 (1) - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

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

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

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

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

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

192.168.64.7 (tcp/80/www)

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

  - HTTP methods GET HEAD OPTIONS POST are allowed on :

    /
```

45590 (1) - 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: 2023/05/31

Plugin Output

192.168.64.7 (tcp/0)

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

  cpe:/o:linux:linux_kernel -> Linux Kernel

Following application CPE matched on the remote system :

  cpe:/a:apache:http_server:2.4.46 -> Apache Software Foundation Apache HTTP Server
```

48204 (1) - 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-0530

Plugin Information

Published: 2010/07/30, Modified: 2023/05/24

Plugin Output

192.168.64.7 (tcp/80/www)

```
URL        : http://192.168.64.7/
Version    : 2.4.46
Source     : Server: Apache/2.4.46 (Debian)
backported : 0
os         : Debian
```

54615 (1) - Device Type

Synopsis

It is possible to guess the remote device type.

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

192.168.64.7 (tcp/0)

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

66334 (1) - 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: 2023/05/31

Plugin Output

192.168.64.7 (tcp/0)

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

[ Apache 2.4.x < 2.4.56 Multiple Vulnerabilities (172186) ]

+ Action to take : Upgrade to Apache version 2.4.56 or later.

+Impact : Taking this action will resolve 29 different vulnerabilities (CVEs).
```

86420 (1) - 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: 2020/05/13

Plugin Output

192.168.64.7 (tcp/0)

```
The following is a consolidated list of detected MAC addresses:
  - 8A:54:CB:45:6A:55
```