My Basic Network Scan

Wed, 11 Feb 2026 13:27:30 CET

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

192.168.122.168

CRITICAL	HIGH	MEDIUM	LOW	INFO
7	2	4	1	112

Scan Information

Start time: Wed Feb 11 13:02:04 2026

End time: Wed Feb 11 13:27:29 2026

Host Information

Netbios Name: VAGRANT-2008R2

IP: 192.168.122.168

MAC Address: 52:54:00:64:7E:B3

OS: Microsoft Windows Server 2008 R2 Standard Service Pack 1

Vulnerabilities

119499 - Elasticsearch ESA-2015-06 -

Synopsis

The remote web server hosts a Java application that is vulnerable.

Description

Elasticsearch versions prior to 1.6.1 are vulnerable to an attack that can result in remote code execution.

See Also

http://www.nessus.org/u?3f00797e

Solution

Users should upgrade to 1.6.1 or 1.7.0. Alternately, ensure that only trusted applications have access to the transport protocol port.

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

5.9

EPSS Score

0.399

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)

References

CVE CVE-2015-5377

Plugin Information

Published: 2018/12/07, Modified: 2019/11/01

Plugin Output

tcp/9200/elasticsearch

```
URL : http://192.168.122.168:9200/
Installed version : 1.1.1
Fixed version : 1.6.1 / 1.7.0
```

105752 - Elasticsearch Transport Protocol Unspecified Remote Code Execution -

Synopsis

Elasticsearch contains an unspecified flaw related to the transport protocol that may allow a remote attacker to execute arbitrary code.

Description

Elasticsearch could allow a remote attacker to execute arbitrary code on the system, caused by an error in the transport protocol. An attacker could exploit this vulnerability to execute arbitrary code on the system.

See Also

http://www.nessus.org/u?c6b6cf1a

Solution

Users should upgrade to 1.6.1 or 1.7.0. Alternately, ensure that only trusted applications have access to the transport protocol port

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

5.9

EPSS Score

0.399

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)

References

CVE CVE-2015-5377

Plugin Information

Published: 2018/01/11, Modified: 2019/11/08

Plugin Output

tcp/9200/elasticsearch

```
URL : http://192.168.122.168:9200/
Installed version : 1.1.1
Fixed version : 1.6.1
```

90192 - ManageEngine Desktop Central 8 / 9 < Build 91100 Multiple RCE -

Synopsis

The remote web server contains a Java-based web application that is affected by multiple remote code execution vulnerabilities.

Description

The ManageEngine Desktop Central application running on the remote host is version 8, or else version 9 prior to build 91100. It is, therefore, affected by multiple remote code execution vulnerabilities :

- A flaw exists in the statusUpdate script due to a failure to properly sanitize user-supplied input to the 'fileName' parameter. An unauthenticated, remote attacker can exploit this, via a crafted request to upload a PHP file that has multiple file extensions and by manipulating the 'applicationName' parameter, to make a direct request to the uploaded file, resulting in the execution of arbitrary code with NT-AUTHORITY\SYSTEM privileges. (CVE-2015-82001)

- An unspecified flaw exists in various servlets that allow an unauthenticated, remote attacker to execute arbitrary code. No further details are available.

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

See Also

http://www.nessus.org/u?89099720

Solution

Upgrade to ManageEngine Desktop Central version 9 build 91100 or later.

Risk Factor

Critical

VPR Score

7.3

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

8.3 (CVSS2#E:F/RL:OF/RC:ND)

References

CVE	CVE-2015-82001
XREF	TRA:TRA-2015-07

Plugin Information

Published: 2016/03/25, Modified: 2019/11/19

Plugin Output

tcp/8022/www

```
URL : http://192.168.122.168:8022/
Installed version : 9 Build 91084
Fixed version : 9 Build 91100
```

90192 - ManageEngine Desktop Central 8 / 9 < Build 91100 Multiple RCE -

Synopsis

The remote web server contains a Java-based web application that is affected by multiple remote code execution vulnerabilities.

Description

The ManageEngine Desktop Central application running on the remote host is version 8, or else version 9 prior to build 91100. It is, therefore, affected by multiple remote code execution vulnerabilities :

- A flaw exists in the statusUpdate script due to a failure to properly sanitize user-supplied input to the 'fileName' parameter. An unauthenticated, remote attacker can exploit this, via a crafted request to upload a PHP file that has multiple file extensions and by manipulating the 'applicationName' parameter, to make a direct request to the uploaded file, resulting in the execution of arbitrary code with NT-AUTHORITY\SYSTEM privileges. (CVE-2015-82001)

- An unspecified flaw exists in various servlets that allow an unauthenticated, remote attacker to execute arbitrary code. No further details are available.

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

See Also

http://www.nessus.org/u?89099720

Solution

Upgrade to ManageEngine Desktop Central version 9 build 91100 or later.

Risk Factor

Critical

VPR Score

7.3

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

8.3 (CVSS2#E:F/RL:OF/RC:ND)

References

CVE	CVE-2015-82001
XREF	TRA:TRA-2015-07

Plugin Information

Published: 2016/03/25, Modified: 2019/11/19

Plugin Output

tcp/8383/www

```
URL : https://192.168.122.168:8383/
Installed version : 9 Build 91084
Fixed version : 9 Build 91100
```

139377 - ManageEngine Desktop Central < 10 Build 10.0.533 Integer Overflow -

Synopsis

The remote web server contains a Java-based web application that is affected by an integer overflow vulnerability.

Description

The ManageEngine Desktop Central application running on the remote host is prior to version 10 build 10.0.533. It is, therefore, affected by an integer overflow condition due to improper handling of header values. An unauthenticated, remote attacker can exploit this, by sending specially crafted HTTP requests, to cause a denial of service condition or the execution of arbitrary code.

See Also

http://www.nessus.org/u?470f5384

Solution

Upgrade to ManageEngine Desktop Central version 10 build 10.0.533 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

5.9

EPSS Score

0.0598

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-2020-15588
XREF	IAVA:2020-A-0350-S

Plugin Information

Published: 2020/08/06, Modified: 2022/05/02

Plugin Output

tcp/8022/www

```
URL : http://192.168.122.168:8022/
Installed version : 9 build 91084
Fixed version : 10 Build 10.0.533
```

139377 - ManageEngine Desktop Central < 10 Build 10.0.533 Integer Overflow -

Synopsis

The remote web server contains a Java-based web application that is affected by an integer overflow vulnerability.

Description

The ManageEngine Desktop Central application running on the remote host is prior to version 10 build 10.0.533. It is, therefore, affected by an integer overflow condition due to improper handling of header values. An unauthenticated, remote attacker can exploit this, by sending specially crafted HTTP requests, to cause a denial of service condition or the execution of arbitrary code.

See Also

http://www.nessus.org/u?470f5384

Solution

Upgrade to ManageEngine Desktop Central version 10 build 10.0.533 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

5.9

EPSS Score

0.0598

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-2020-15588
XREF	IAVA:2020-A-0350-S

Plugin Information

Published: 2020/08/06, Modified: 2022/05/02

Plugin Output

tcp/8383/www

```
URL : https://192.168.122.168:8383/
Installed version : 9 build 91084
Fixed version : 10 Build 10.0.533
```

108797 - Unsupported Windows OS (remote) -

Synopsis

The remote OS or service pack is no longer supported.

Description

The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.

See Also

https://support.microsoft.com/en-us/lifecycle

Solution

Upgrade to a supported service pack or operating system

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-0501

Plugin Information

Published: 2018/04/03, Modified: 2025/10/21

Plugin Output

tcp/0

```
The following Windows version is installed and not supported:

Microsoft Windows Server 2008 R2 Standard Service Pack 1
```

Synopsis

The remote web server contains a Java-based web application that is affected by a remote privilege escalation.

Description

The ManageEngine Desktop Central application running on the remote host is version 10 prior to build 100282. It is, therefore, affected by a remote privilege escalation vulnerability.

See Also

http://www.nessus.org/u?ddf441fc

Solution

Upgrade to ManageEngine Desktop Central version 10 build 100282 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0386

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

BID	105348
CVE	CVE-2018-13411
CVE	CVE-2018-13412
XREF	IAVA:2018-A-0302-S

Plugin Information

Published: 2018/09/21, Modified: 2024/08/06

Plugin Output

tcp/8022/www

```
URL : http://192.168.122.168:8022/
Installed version : 9 build 91084
Fixed version : 10 Build 100282
```

Synopsis

The remote web server contains a Java-based web application that is affected by a remote privilege escalation.

Description

The ManageEngine Desktop Central application running on the remote host is version 10 prior to build 100282. It is, therefore, affected by a remote privilege escalation vulnerability.

See Also

http://www.nessus.org/u?ddf441fc

Solution

Upgrade to ManageEngine Desktop Central version 10 build 100282 or later.

Risk Factor

High

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

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

VPR Score

6.7

EPSS Score

0.0386

CVSS v2.0 Base Score

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

CVSS v2.0 Temporal Score

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

STIG Severity

I

References

BID	105348
CVE	CVE-2018-13411
CVE	CVE-2018-13412
XREF	IAVA:2018-A-0302-S

Plugin Information

Published: 2018/09/21, Modified: 2024/08/06

Plugin Output

tcp/8383/www

```
URL : https://192.168.122.168:8383/
Installed version : 9 build 91084
Fixed version : 10 Build 100282
```

101025 - Elasticsearch Unrestricted Access Information Disclosure -

Synopsis

The search engine running on the remote web server is affected by an information disclosure vulnerability.

Description

The Elasticsearch application running on the remote web server is affected by an information disclosure vulnerability due to a failure to restrict resources via authentication. An unauthenticated, remote attacker can exploit this to disclose sensitive information from the database.

See Also

http://www.nessus.org/u?d055e692
http://www.nessus.org/u?b80612a1

Solution

Enable native user authentication or integrate with an external user management system such as LDAP and Active Directory.

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: 2017/06/23, Modified: 2017/06/27

Plugin Output

tcp/9200/elasticsearch

```
Nessus detected an unprotected instance of Elasticsearch with the following indices :



5
```

108752 - ManageEngine Desktop Central 9 < Build 92027 Multiple Vulnerabilities -

Synopsis

The remote web server contains a Java-based web application that is affected by multiple vulnerabilities.

Description

The ManageEngine Desktop Central application running on the remote host is version 9 prior to build 92027. It is, therefore, affected by multiple vulnerabilities including a remote code execution and three cross-site scripting vulnerabilities.

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

See Also

http://www.nessus.org/u?b2a97375

Solution

Upgrade to ManageEngine Desktop Central version 9 build 92027 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

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

VPR Score

3.0

EPSS Score

0.0187

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

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

References

CVE CVE-2018-8722

Plugin Information

Published: 2018/03/30, Modified: 2019/11/08

Plugin Output

tcp/8022/www

```
URL : http://192.168.122.168:8022/
Installed version : 9 Build 91084
Fixed version : 9 Build 92027
```

108752 - ManageEngine Desktop Central 9 < Build 92027 Multiple Vulnerabilities -

Synopsis

The remote web server contains a Java-based web application that is affected by multiple vulnerabilities.

Description

The ManageEngine Desktop Central application running on the remote host is version 9 prior to build 92027. It is, therefore, affected by multiple vulnerabilities including a remote code execution and three cross-site scripting vulnerabilities.

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

See Also

http://www.nessus.org/u?b2a97375

Solution

Upgrade to ManageEngine Desktop Central version 9 build 92027 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

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

VPR Score

3.0

EPSS Score

0.0187

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

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

References

CVE CVE-2018-8722

Plugin Information

Published: 2018/03/30, Modified: 2019/11/08

Plugin Output

tcp/8383/www

```
URL : https://192.168.122.168:8383/
Installed version : 9 Build 91084
Fixed version : 9 Build 92027
```

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

http://www.nessus.org/u?df39b8b3
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 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)

Plugin Information

Published: 2012/01/19, Modified: 2022/10/05

Plugin Output

tcp/445/cifs

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

VPR Score

2.2

EPSS Score

0.0037

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 ICMP timestamps seem to be in little endian format (not in network format)
The difference between the local and remote clocks is -98 seconds.
```

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.

NOTE: When paranoia levels are elevated, this plugin will also consider versions obtained from responses with non-200 HTTP status codes.

See Also

https://tomcat.apache.org/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0535

Plugin Information

Published: 2009/06/18, Modified: 2025/05/15

Plugin Output

tcp/8022/www

```
URL : http://192.168.122.168:8022/
Version : unknown
```

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: 2026/01/05

Plugin Output

tcp/0

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

cpe:/o:microsoft:windows_server_2008:r2:sp1 -> Microsoft Windows Server 2008

Following application CPE's matched on the remote system :

cpe:/a:apache:tomcat -> Apache Software Foundation Tomcat
cpe:/a:elasticsearch:elasticsearch:1.1.1 -> Elasticsearch
cpe:/a:oracle:glassfish_server:4.0 -> Oracle GlassFish Server v
cpe:/a:smartbedded:meteobridge_firmware
cpe:/a:zohocorp:manageengine_desktop_central:9 -> ZohoCorp ManageEngine Desktop Central
```

10736 - DCE Services Enumeration -

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) 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/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/135/epmap

```
The following DCERPC services are available locally :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc040C40

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WindowsShutdown

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc040C40

Object UUID : 6d726574-7273-0076-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : LRPC-b667ae12f9d50b829b
```

```
Object UUID : 52ef130c-08fd-4388-86b3-6edf00000001
UUID : 12e65dd8-887f-41ef-91bf-8d816c42c2e7, version 1.0
Description : Unknown RPC service
Annotation : Secure Desktop LRPC interface
Type : Local RPC service
Named pipe : WMsgKRpc041E31

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000001
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : WMsgKRpc041E31

Object UUID : 8b71de69-a415-49f2-8bc1-8c9b4b3afc6c
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC-9c86f54c4c5319ded6

Object UUID : ce85ca4c-c120-4948-91c4-43be6fd79eca
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC-9c86f54c4c5319ded6

Object UUID : 0588f7be-ed5d-41f9-b125-4f308f1dde95
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC-9c86f54c4c5319ded6

Object UUID : 1176ae5d-41a1-4a00-9286-b6b1ae7acf03
UUID : 906b0ce0-c70b-1067-b317-00dd010662da, version 1.0
Description : Distributed Transaction Coordinator
Windows process : msdtc.exe
Type : Local RPC service
Named pipe : LRPC-9c86f54c4c5319ded6

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
Description : IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Annotation : IPSec Policy agent endpoint
Type : Local RPC service
Named pipe : LRPC-4d4ec2da2b46c30fcf

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : LRPC-73a6a5503ec0194bbb

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : audit

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : securityevent

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : LSARPC_ENDPOINT

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : lsapolicylookup

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
```

```
Type : Local RPC service
Named pipe : lsasspirpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : protected_storage

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : dsrole

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Local RPC service
Named pipe : samss lpc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1.0
Description : Unknown RPC service
Annotation : Spooler function endpoint
Type : Local RPC service
Named pipe : spoolss

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : ae33069b-a2a8-46ee-a235-ddfd339be281, version 1.0
Description : Unknown RPC service
Annotation : Spooler base remote object endpoint
Type : Local RPC service
Named pipe : spoolss

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 4a452661-8290-4b36-8fbe-7f4093a94978, version 1.0
Description : Unknown RPC service
Annotation : Spooler function endpoint
Type : Local RPC service
Named pipe : spoolss

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : dd490425-5325-4565-b774-7e27d6c09c24, version 1.0
Description : Unknown RPC service
Annotation : Base Firewall Engine API
Type : Local RPC service
Named pipe : LRPC-5aafca618a206d9765

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-5aafca618a206d9765

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 2fb92682-6599-42dc-ae13-bd2ca89bd11c, version 1.0
Description : Unknown RPC service
Annotation : Fw APIs
Type : Local RPC service
Named pipe : LRPC-5aafca618a206d9765

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7ea70bcf-48af-4f6a-8968-6a440754d5fa, version 1.0
Description : Unknown RPC service
Annotation : NSI server endpoint
Type : Local RPC service
Named pipe : OLE2479077D5BCC49E1B9A3898FB86A

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 7ea70bcf-48af-4f6a-8968-6a440754d5fa, version 1.0
Description : Unknown RPC service
Annotation : NSI server endpoint
Type : Local RPC service
Named pipe : LRPC-f626d5a3d44be1fbf0

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Local RPC service
Named pipe : OLE2479077D5BCC49E1B9A3898FB86A

Object UUID : 00000000-0000-0000-0000-000000000000
```

```
UUID : 3473dd4d-2e88-4006-9cba-22570909dd10, version 5.0
Description : Unknown RPC service
Annotation : WinHttp Auto-Proxy Service
Type : Local RPC service
Named pipe : LRPC-f626d5a3d44be1fbf0

Object UUID : 666f7270-6c69-7365-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 6c637067-6569-746e-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 24d1f7c7-76af-4f28-9ccd-7f6cb6468601
UUID : 2eb08e3e-639f-4fba-97b1-14f878961076, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : OLEF594C39F3B33482BABC689AD319B

Object UUID : 736e6573-0000-0000-0000-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLEF594C39F3B33482BABC689AD319B

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLEF594C39F3B33482BABC689AD319B

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : senssvc
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : OLEF594C39F3B33482BABC689AD319B

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEF594C39F3B33482BABC689AD319B

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Local RPC service
Named pipe : OLEF594C39F3B33482BABC689AD319B

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Local RPC service
Named pipe : OLEF594C39F3B33482BABC689AD319B

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Local RPC service
Named pipe : IUserProfile2
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Local RPC service
Named pipe : OLEF594C39F3B33482BABC689AD319B

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Local RPC service
Named pipe : senssvc

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : OLEF594C39F3B33482BABC689AD319B

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : IUserProfile2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : OLEF594C39F3B33482BABC689AD319B

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Local RPC service
Named pipe : senssvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Local RPC service
Named pipe : eventlog

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Local RPC service
Named pipe : eventlog

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Local RPC service
Named pipe : eventlog

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Local RPC service
Named pipe : dhcpcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
```

```
Type : Local RPC service
Named pipe : eventlog

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Local RPC service
Named pipe : dhcpcsvc

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Local RPC service
Named pipe : dhcpcsvc6
```

10736 - DCE Services Enumeration -

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) 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/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/445/cifs

```
The following DCERPC services are available remotely :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\VAGRANT-2008R2

Object UUID : b08669ee-8cb5-43a5-a017-84fe00000000
UUID : 76f226c3-ec14-4325-8a99-6a46348418af, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\InitShutdown
Netbios name : \\VAGRANT-2008R2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \pipe\lsass
Netbios name : \\VAGRANT-2008R2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
Type : Remote RPC service
Named pipe : \PIPE\protected_storage
Netbios name : \\VAGRANT-2008R2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 1ff70682-0a51-30e8-076d-740be8cee98b, version 1.0
```

```
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\VAGRANT-2008R2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 378e52b0-c0a9-11cf-822d-00aa0051e40f, version 1.0
Description : Scheduler Service
Windows process : svchost.exe
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\VAGRANT-2008R2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\VAGRANT-2008R2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\VAGRANT-2008R2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\VAGRANT-2008R2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\VAGRANT-2008R2

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\VAGRANT-2008R2

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
Named pipe : \PIPE\srvsvc
Netbios name : \\VAGRANT-2008R2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\atsvc
Netbios name : \\VAGRANT-2008R2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
Named pipe : \PIPE\srvsvc
Netbios name : \\VAGRANT-2008R2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\VAGRANT-2008R2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Remote RPC service
```

```
Named pipe : \pipe\eventlog
Netbios name : \\VAGRANT-2008R2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\VAGRANT-2008R2

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
Named pipe : \pipe\eventlog
Netbios name : \\VAGRANT-2008R2
```

10736 - DCE Services Enumeration -

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) 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/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49152/dce-rpc

```
The following DCERPC services are available on TCP port 49152 :

Object UUID : 765294ba-60bc-48b8-92e9-89fd77769d91
UUID : d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49152
IP : 192.168.122.168
```

10736 - DCE Services Enumeration -

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) 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/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49153/dce-rpc

```
The following DCERPC services are available on TCP port 49153 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1.0
Description : Unknown RPC service
Annotation : Event log TCPIP
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.122.168

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1.0
Description : Unknown RPC service
Annotation : NRP server endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.122.168

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1.0
Description : DHCP Client Service
Windows process : svchost.exe
Annotation : DHCP Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.122.168

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1.0
Description : Unknown RPC service
Annotation : DHCPv6 Client LRPC Endpoint
Type : Remote RPC service
TCP Port : 49153
IP : 192.168.122.168
```

10736 - DCE Services Enumeration -

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) 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/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49154/dce-rpc

```
The following DCERPC services are available on TCP port 49154 :

Object UUID : 00000000-0000-0000-0000-000000000000
```

```
UUID : 86d35949-83c9-4044-b424-db363231fd0c, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.122.168

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1.0
Description : Unknown RPC service
Annotation : IKE/Authip API
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.122.168

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1.0
Description : Unknown RPC service
Annotation : IP Transition Configuration endpoint
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.122.168

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1.0
Description : Unknown RPC service
Annotation : XactSrv service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.122.168

Object UUID : 73736573-6f69-656e-6e76-000000000000
UUID : c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1.0
Description : Unknown RPC service
Annotation : Impl friendly name
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.122.168

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1.0
Description : Unknown RPC service
Type : Remote RPC service
TCP Port : 49154
IP : 192.168.122.168
```

10736 - DCE Services Enumeration -

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) 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/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49180/dce-rpc

```
The following DCERPC services are available on TCP port 49180 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345778-1234-abcd-ef00-0123456789ac, version 1.0
Description : Security Account Manager
Windows process : lsass.exe
```

```
Type : Remote RPC service
TCP Port : 49180
IP : 192.168.122.168
```

10736 - DCE Services Enumeration -

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) 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/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49181/dce-rpc

```
The following DCERPC services are available on TCP port 49181 :

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 367abb81-9844-35f1-ad32-98f038001003, version 2.0
Description : Service Control Manager
Windows process : svchost.exe
Type : Remote RPC service
TCP Port : 49181
IP : 192.168.122.168
```

10736 - DCE Services Enumeration -

Synopsis

A DCE/RPC service is running on the remote host.

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) 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/pipe.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/08/26, Modified: 2021/10/04

Plugin Output

tcp/49210/dce-rpc

```
The following DCERPC services are available on TCP port 49210 :
```

```
Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1.0
Description : Unknown RPC service
Annotation : Remote Fw APIs
Type : Remote RPC service
TCP Port : 49210
IP : 192.168.122.168

Object UUID : 00000000-0000-0000-0000-000000000000
UUID : 12345678-1234-abcd-ef00-0123456789ab, version 1.0
Description : IPsec Services (Windows XP & 2003)
Windows process : lsass.exe
Annotation : IPSec Policy agent endpoint
Type : Remote RPC service
TCP Port : 49210
IP : 192.168.122.168
```

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 : 99
```

109941 - Elasticsearch Detection

Synopsis

The remote web server is running a distributed search engine.

Description

The remote host is running Elasticsearch, a distributed search engine service written in Java and possibly a security extension called X-Pack.

Note that HTTP Basic/Digest credentials may be required to retrieve version information.

See Also

https://www.elastic.co/products/elasticsearch

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2018/05/21, Modified: 2026/01/05

Plugin Output

tcp/9200/elasticsearch

```
URL : http://192.168.122.168:9200/
Version : 1.1.1
```

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:
- 52:54:00:64:7E:B3
```

43111 - HTTP Methods Allowed (per directory) -

Synopsis

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

Description

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

The following HTTP methods are considered insecure:
PUT, DELETE, CONNECT, TRACE, HEAD

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

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

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

See Also

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

http://www.nessus.org/u?b019cbdb
https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8022/www

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

- HTTP methods DELETE HEAD OPTIONS POST PUT GET
are allowed on :

/
```

43111 - HTTP Methods Allowed (per directory) -

Synopsis

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

Description

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

The following HTTP methods are considered insecure:
PUT, DELETE, CONNECT, TRACE, HEAD

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

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

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

See Also

http://www.nessus.org/u?d9c03a9a
http://www.nessus.org/u?b019cbdb
https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8080/www

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

- HTTP methods DELETE HEAD OPTIONS POST PUT TRACE GET
are allowed on :

/
```

43111 - HTTP Methods Allowed (per directory) -

Synopsis

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

Description

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

The following HTTP methods are considered insecure:
PUT, DELETE, CONNECT, TRACE, HEAD

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

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

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

See Also

http://www.nessus.org/u?d9c03a9a
http://www.nessus.org/u?b019cbdb
https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8181/www

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

- HTTP methods DELETE HEAD OPTIONS POST PUT TRACE GET
are allowed on :

/
```

43111 - HTTP Methods Allowed (per directory) -

Synopsis

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

Description

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

The following HTTP methods are considered insecure:
PUT, DELETE, CONNECT, TRACE, HEAD

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

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'
in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

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

See Also

http://www.nessus.org/u?d9c03a9a
http://www.nessus.org/u?b019cbdb
https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

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

Plugin Output

tcp/8383/www

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

- HTTP methods DELETE HEAD OPTIONS POST PUT GET
are allowed on :

/
```

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/3000/www

```
The remote web server type is :

WEBrick/1.3.1 (Ruby/2.3.3/2016-11-21)
```

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/4848/www

```
The remote web server type is :

GlassFish Server Open Source Edition 4.0
```

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/5985/www

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

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/8022/www

```
The remote web server type is :

Apache-Coyote/1.1
```

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/8080/www

```
The remote web server type is :

GlassFish Server Open Source Edition 4.0
```

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/8181/www

```
The remote web server type is :

GlassFish Server Open Source Edition 4.0
```

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/8383/www

```
The remote web server type is :

Apache
```

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/8484/www

```
The remote web server type is :

Jetty(winstone-2.8)
```

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/3000/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 : GET,HEAD,POST,OPTIONS
Headers :

X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Type: text/html; charset=utf-8
Etag: "9fdff472a0cc0802ae8009cd2322f2da"
Cache-Control: max-age=0, private, must-revalidate
X-Request-Id: 5d70da81-3144-4d1c-96ff-327b4dd0adfd
X-Runtime: 0.000000
Server: WEBrick/1.3.1 (Ruby/2.3.3/2016-11-21)
Date: Wed, 11 Feb 2026 12:09:32 GMT
Content-Length: 14846
Connection: Keep-Alive

Response Body :

```
<!DOCTYPE html>
<html>
<head>
<title>Ruby on Rails: Welcome aboard</title>
<style media="screen">
body {
margin: 0;
margin-bottom: 25px;
padding: 0;
background-color: #f0f0f0;
font-family: "Lucida Grande", "Bitstream Vera Sans", "Verdana";
font-size: 13px;
color: #333;
}

h1 {
font-size: 28px;
color: #000;
}

a {color: #03c}
a:hover {
background-color: #03c;
color: white;
text-decoration: none;
}


#page {
background-color: #f0f0f0;
width: 750px;
margin: 0;
margin-left: auto;
margin-right: auto;
}

#content {
float: left;
background-color: white;
border: 3px solid #aaa;
border-top: none;
padding: 25px;
width: 500px;
}

#sidebar {
float: right;
width: 175px;
}

#footer {
clear: both;
}

#header, #about, #getting-started {
padding-left: 75px;
padding-right: 30px;
}


#header {
```

```
background-image:
url(
AGZhJREFUeNqsWwmUXGWV/t5Sr9aurl6qO0l3Z9/DEoJh18gZQGAUxPHIyQHH7eioZ8bjnAFHZ0RndNxxRBhGcUbxoKIHBkTEcUYREIHIGpKQjUDS6U660/tS
VV3Lq/fefPf/Xy2dBFGYx3npqvde/e/e/97v3u/e/8e4Lt2L8DCCAFcGwF8ZBjYbgM1rAZoO+WLwZhDMu9y4+YcOozbAqzwXNA3GdzX/5hV+KnKO2+GXFj/Av
zmW8e72iG202CYiphbY403f9/k3QHZtJ9oWtyCQe7wGX79TKVb7rP9pXJPDVxf0Rz+oyxm4HNWrahFNixdk3EAJbERMWOm4ulctVODNVeEVK0DeRVDgb1wfJg
cqUo6duaKnFOH7bm6JmH+5LOEgZprwRIHAV3JYfLjKM55Noz3bBqdcgt0Wg52Kq/cHHkXns0qIukKBlltk9rU2QaiouiefPQ+RdBuseAJeqYTK1CTH8mE4Nsy
IpRWu8nssCs+xULWpjGVwTvieKl/sV6mIXzOib/OftzuG8d6l8SiVMODyRb46oazg8YPP2Wnvy9ISNqplzsxYAW6hjGhHEmYiBoPC+hRMfFMrESgrBC5n0KS+
lq1nPahZh2OXymg9bSNWX/u3FKyKI//7Exx96B4Y8RiCEseq8t0VznyxjMDidFIJ8QSf3hJEOFbZEAHVhIkFTX54fxtnIW5pJUQIeZ8ooZShkInuDOLpFIX1l
dtCBix7KI/k4E7OwbTjcNIdiCQzsONp2LEk7GgUnZsuQN9lW2En45xlukrUghWzeZq8FsXsi8+gND6MSCqD9k3nwulIUShKZxt0LYPWortRSY0NXreC8J6pZN
DChEDh53PT1NIPLaEnLbQKNTETEaR7sycA0jD1INXZAnzObjTbiWh7Vr1A3Knn4nciu+lCvstUig09cp96cVCtcELoFpEIFUjjyIM/osWIg+IMXS3DcfNwZ3N
QHmmKU9OqroX2jWdgatduuPkpmA4ViZrK9RqKABEBtg9tDeW+oUIyTIYuFaX7eCG4aqbU+hhKocD3UBoZISBLiC9cpAQKyq5SQo6OjVswtec5VHLTiHUuIN4W
onXlqUj2riS0DIUXwZlERFHSK+SQGzqI3MHdmNm7CzMvvowF527B8qvejZ3/+iXk9vVTao5tiTKN0OUHISZEGS/8W6UbRdoTSHe3E1f+CRaR3xhBLVJSIQ7ql
eZQGBigZYoYdR+ElUjBaW3H6JMPIrV0Hdo2bEayZ7my0KsdLctPBS64EuWZMYw/9wTGnvod0mtzWH71Vuz66o10bVpK8FIx6orUMejpCKYBTvfM9HXBJtA8z3
/1BKDivaksVJmaYsgsYPDnd6LzzAuw8I1XUIGleC1HtDWLnguv5BiX4+jDD2D4sQeV1bQvNXBi6vAb1MGtrEEHjRPgqfZ0qMRJElYYSudfq12nmzAvtJ2yib6
9iRadRGnySD0Uv5bDtCPou/gqnPY3N6DnLRczgtHxCf4aVnUeUdgw6i6FqM1w292Ujo/TJdB5wHcJ2iDCaBTRmVfw4rkw4yksuvQyJJf0YvrgNiayvBLESS9A
YuFqJLLLCPb4SQWulosojhxmeCeoDeaQSoVuy8lPtSKxYKnC2Bmf+DwtvBgv3/qfTI6uEtGuJV7PCBTIq5zNtt5uxBgyvap30pf55TISfX1Y/PatGPrVvcgPv
EyAJ1GenaPZLSy//G2IL+qki43CNCMwk620iovy9FGUJgYwm8gwpK/guRJOS5dyD688h+n9z2L28F4Ujx2ia04jEl8Ad3oGVTePaGcnQ3sKLb1rkD3nIqx594
dRIh733n6PmmrrvGj671sjVlxczRWAkxZ0r+rTrhfMJ0uEM8xKUYXONR+5nr57BdpP24TCsX6M/f5F5AYLWPauK9F11htUwjOIL8GNZH1qpKwiyVGELk0OoDj
2EtziFOaODSN3aC/v24xmZzAU51TgcJKd/DktHo9jyRXvg0Or7PvejTj22KPKiyafew6zg8MYypVLNsLkJ2bxaZXM4i5EmCBPsEaoWJUUpfeSK7DgvEtQmh4i
hTDQdf5FOHDHr7HqPVeh99KL4OVzpE50N18CtqnCdBCY6rsEcTsqIGUGD6rY9e3bMPzIHmTWLsbqa7ai84wL6YrTqEyOqEmwonEExSoO//R7dLcJWiWCueF+7
P7mjZAUY8YdJZqySMo24j5zQSybQdeyhdrX5imho4NhEEnkRbkDQyjSRVJLeziCgef/6avIrFuOtR95P2lJNSSshg4l6rdm+Ht9inWsqIOX7voN+u/eRoEM5P
vHMbbjGcwcfg7jO3YxbCcRiaaYQOXnpEaFGeahGQaMCidJRidt8RghS6Q344XQIowmFq2QXdLNdwsx8zUFqCOQNIECVqdp8pESB53Fvhdux9T2FxBb1AWX4Xb
jDX/HFzjEmgedB4XYKT5D4T0VTLRCtIiTwOBvfovpvS8T+Bm4MyW6jw13tIIDt/9G/TTWk8HKvzgbmd4+YldYQIdixgHJYkC82Ul6UDnQSbEGdsFGZlEWyUyL
yiEyYwajRVAoAXNlEjR+pjUCUmiDQcKOORwwgpFfP4cg5mPzTZ9FoqePdGVWuZRPYQNPcgrd0/dCpqpdy3DIsQ4fxtiTu7Hxkx8iRXkcB+94iM86/K0Jx4opi
5aOzGJs14toWeLAdYXWxFQCtJlkA+LUq+bI7QR3mj3YoqVNgGcXd5NWUOiZAk9GH86S4jK25jWBLVREl1uK5Voywz6WXf1WLHjTm0lPigSyxoUpnEqU8c26Wy
k/Y24RMjhw/yMoj+cQbWvH0isuwuijL6BwaJwcyq7XUTaBP7N3HOU3ke7HSONJb8RTBGoGKZPFyTE8saTZyCPtrC2coxOoTuY5+x4UTzHNsNjR6d6Qa8JJ5BI
V8ksVtKzpwcr3v5dyOrzHKMWXizsZAnK6k1ImPDmAqjOmdr9AwXcodzr4kwfQfuY6VKbzyhpGU96S75WxIqb2DaPnvNWKklQD4WSuzB+sVILjOYjm/VARSWKT
BQQzlZCFmErYeubzVJJR14SlQtVQMjO0xrXvoulXkq3OKnxAXqSsoSmNUbOM/BV35RjDDz9JrBXpnnEM3vsYjj38LLyZihI8QNAgQhITOCmTO46i+6w1MPm86
RVIiC09/RJUGcECCe2UU0G6QIyUjEC5hGaCNd4RqHKU6VuDylQlI2N8hfXDWibEdyhCKXREuZUVUX8lyhh2+Jl5Q/6akSgT4izGn3wBFu+JwYOKj8qwtsbJaY
mJuYEZ5AYmFOWXPCN1jTodzeuqM0WtSI1rzXrV0LSNKRFuZLYQ2EYVPjEQVuQUMsCya65GvL1HWUwJS+FNUcBsUiZUQv7aLGlndr+I8ug4XUMVAJw4U7FmI8S
FETTmUaGK2gas1SeeP8znoizIEso9DaUIy2FWkNU5V0VYs/azWXKncuCHqgQq1CHiY831H8TGr34erRvXKdD6LD3b+HnRn12qGgdqlmxHZe2aRcy6NbQScl8y
8dSOfWQE1yK9YYmqXYww3xhNObemUI2IWraF2d1HMTeeh83MbkUiylKiiMdy2wjzXBjxWYdRiSkhfDVVKGSstxM9l16JxZe/E2+848c49bPXK9D2vPUyEsBOV
ZMINmpCW6HgEOuIQjXF6FYuAV2aHsWyrVfj9C9er5SR5Kms0PTf8QoZtIo7WSJW+mmRJLGSpDK2ipzV2bK6X6fxtWOCicYVqyhGXkXn+WeTcfape5ZDsPGM91
C5iy8LI0s445bd9FkrAFHICt1N8DE+gdyeQczs34+uzeei68LNLGfdea50st6VbiyYmHq+nxTFRSSRVsD3ii7xyeQbdt/M5h/MERMT4i6GjlAWeUxh6HCN8+L
Iz+5H5zlUbtHSOnVp4MCa51JaIQ16i0kwP9CP0uExPP+JL2DggfuYN8jTJClYxnH4aNimdpp0r7nDkyx9h5gE0+RqSVTyZXXTsMz5FaJyMJrrGLNopyWUIImj
//1LjPzuUZLCC5gzVqMwPIglV7/rxCaihFaCPCDOxDUl1EoylFP4mUlFCgPDStLKWB47PnUjrSSsNqrJsa/zR02ZwGjYRoVkEZh0ZHzbfmTPXE85SWrnKip6G
eFE2I1iKVBCzNK9pmiVhS1x+Axx7myRJesvgHvvR3rNKmQ3n/OKPVGND1MVXTqHiFK6qVFiwlXgTVDhkq+ChhnyJCW9GeaoIGQOdV0M9YhYZWbvUXrIJJ+rKL
6lJ9CYj5Fai0iKqyPkx0HcUsJYrBbtREIJ2H72GxTI/2CL1zAbLkZ8WIxYgUvsKebq6Zl3rEZvymx6echo1N+au9XcS3oHsxWMPrGTFH+CLhsmbhMNRWrNB4S
ZVSwyJ5WDFRb3DAAmaXf2rPP+6BpbkmStkBLAWwkHmdNWKfYqFaZRp2GGdo+mhpv6bBkNhepRzERpdASeW1aKSZ5RidpoUsRAvQ+NJCnJHHl+bcZ80vjkij66
1vo/rWMQSitWskgnNv7LP+MNN38NadYuCPtYCItIFTjMRgfeqClkhkFZ+FXCQmpFuyKXii7xNI93LT9szdrUMsNZnJkuwZX6zlKdaqRXrESiq/e19kBC3NisL
t+Gc/7jW0gtZ51Bl1MCmUaoM//aRv0aapnF0l362KIUnI6EyuhCUOuWrIVfAZcRAj5NJWJ0C5epP19y1awJLWhdt/a1t3KcGF8Yxb5bbsLItoeYmxZRkRWq46
IrR9StX/tcw4oKsYH+nlrZpmbcZQ7R1tDPBvMbdIwofLpVKIfcJy5nCa5WRhnDFkVOx+s5kr29GPzpfUxsuxg0zlQUxSZudG/CqNOSIJxYCclGCA7fDRDpiCK
6gIVfidVmWXrHRh0fmBd+eSYIIEcWdRhdJJsWp+aQT1vI9nYjnl3wuhSJLuhAJJ1WQWDisadUELCi0bD1WlscMpq6lrV1Ft0riC9tVcFD8odfDVS9bod5pNGg
C3+XFnxsXA2rsw25/gHMTcwiRxdbvLgPsY7s61IktWSZinw6l8SbupNGvUlphB1yZY3aIhfZtRmz4XS3oMoA5JP6BywdvBIr24ytMdzsWjHaMcnI0nXRG5Fkd
CrnS6gy6QzccxeMZDsJW+r1KbJ4pbKAVy6huXoyauVUaAUjRK5WjN9cH05PCiZl84VfsXaSVTKf191C6F61qCXjtjAORtvTSPb0sgYoEi/UmEmnMj6JkpXA6z
2cTAbxxV26GdEEZB12DVVV63BrIuwYaWpCGZyuJBWSFSxPLTB5PH1+rhDDKlQbuvajNUzE+UVyRTTdQt+zWIrGWIJOozo8hjmashq8PkXsZAoty1Yqi/gVnq6
ru+p1pUKFTM3dENJzu421TiqKKq3hhUp45apSyM1VGMH0xOi+liz0yOxUyijs2w2DlRjI+8tHB3XUIP+fGBxA9+LFr1kRgwV769p1fPkEQ+9KRq+dKE9MsGKc
1BmxltEC7W6CEdW0aUtocIvw0tcSt5JGu3R4OA+zIxW1uKoUOUZzFxmxRp/ai+iz+xi9CK5EVJGdqBNBlG4xdvBlRq9eTQteawhm0MgPLsSGj92gVqjKk8ew/
TOfxPjjz8BKxhvLFGHjWUBuJh0Cu6pqD7WCTGz4BDqKpE30rIlj05rw6sKFxuCXPP9O8MEjxQqOTuQwNjJLa1mItaRRGB3GLHnO6znaNmxC/nA/cocPKNoS61
iEZVdfEy5LBHVKUieCLY5eeKIiXp6RapJuNVJFMCamYGnOUFyslBo0Xronai0dIfXmnZIqtKhgNIaj/F3ULSLx4j60dnXXy8s/OZe0dyGW7cLOL34arevXI9r
ayWgYhZPtoJtNqsTbyPKUgwzamyCw867MtG5NBUF9bSBXLCkeKOzDroUutaZODax52yUk5sfgsyrL897+PXtQHTmK7vWnomPpCkSTf3pI7j7/Qmz/5HWY3r5L
NziYeC3WPlYsovOJJ7VKVbuPENcgXEyvuV3IbKXpPlcqqh0acqGe2S1oq1jzqmZ+b0mGDJNaM2bnjrHuPnYUifZOtDMKda9ah1RnZ30F99WO9jM2MzouZw0vL
dJIuCsiUInOz0vbiVNa9DSBtITyWo3VAV/XG/KmPEuBKrmard7rNxKiyCoN7EBnpXlLCiYTmfibuEHSSSkLV4uzGNr5NEYP7EZb31J0rd6AzMIevtf+g4oIg+
7e8iYM3H03J5muw9n3ZquqfwU3aGDdMBqdztr+lXBbhyg+R2xYTb5jN7YG6SKnyh870r8Ki6Py0CiO3fcTNWaCBU3E8FVDr7ZPRjbcDLHO30N/TmazdLk+JFM
xVoZh6errUrcmnDQp5o4MocrI4o3N6dmXhp1hoHkOFV2R5CXtVwm3Qc0aBip8Z6lY0HtRpJ8GYz5pVFgxgkaHiaCuDE1gfOAhFdNbJIKxplCKNJqqyoqi0CT9
tp9/IyyPE2SryYyDKD9LVKxKUqXbuFOM+yVDN/Rq+0ia1mLmtYNqK8rhTiSpLLNbLkDLuZvQ0X8QBoG+//5fIMjP4AQ/kJkuM+vW+sS1wkgiVSTi0Fq2XqoLF
fFYMMkyHSFL2mOpHQmy+aU4xXHoLk6rrIkYiE1JNpZOJjO1ivduOLSkZeuk6/YBwR54jaVv6chXpmZQmJnEssveQjwVcPCXv1IWt4//sUVB7K4WpGTREqhvJC
rO5MhtGLMTKWU5pUSpDKs1glhbB4W3VCSpTM6gOl2GQzxJt+RQUMFcOoENrXG0FEhESSvMmIVIZ6uaHL9QZn6Y067VNJueV4bdmYDdktJ7pAJNKKfG+pG/cz8
GH/gfGLIARF4o9fs8RWSrUmZxN7Z+9za0sooTPiRuI22bsUMHsevWW1B+iFnYdOgqFWTPPxWnXPdxtK5eV8fB9IH92Pn1m1hz7MQh00Xm/C34+K23MiOXsPvL
X8bgbXej5bz1OPs7tzIhduHgnXfghX/8OplEsr6U4ZtV9G69HMvf8wEkKUfgaUeWbs4zX/8Sxm/+AbzxCRVF1VpFM9hrvS2ZmZbuRUh2LpxPw7t60EWK8vgHP
oCZ5w4i1pvBps99Bu2nbJ73XLyzB4kvLcAPt27F2LFR9MTjSKbb1L1h4mIq4iNL14u2ZRFJysazZCNHqA0DZXRcuBGnf+bz6v4JLDqVgk3r247DnMdJDkOzff
JtDfoY2b0dg08/gbZlq7BiyyWk+MuQ2bAGU9v2snTtQnxBj3pu9OnfYXr/Hiq1EZ0bz0ZsUS+sFUvgDB+DFfh1v3X9Kg4xknfLRNZ21h2/RYTX29avU0pUSwU
cuP07KLw0oBZrA5bGozt2MlA5updgzGuJnYyp6rt7778HP37fX+OJW77ZaKzKoo5eOdfRhMehO3+EbXzu8H/dXW/SOTwj0gZqeoVck+h3xES9LDjpVp3QXeRd
qSVLkDllrepy5oeHMPH0brq2qdteRmNJwj7pYKFVlr75YrztKw6ya9aFTzF8Tk+pBZrmXRGRdCsSLMiQbKlfE7PLrjarCcSSA0Q2vQQevGKncnrfXpVwZTde3
+XvqN9b8d4PYfuNn8O+b9zO56K6oGpOiMYreNfSc7eoE+FO00P334XJx3fQzM685zd8/Hqs/uCHGGEy9QEslaT0Cm9t7rVyYqnGWogEGIl+nqUTmyxwTj62HT
s/91ks3XqN2u8VBLKZoVt14pe/42oc/O6dzB2+qnEMNGHEPHHbSfiSqloakGP7D7+Dpz79BfT6cRXu5rHatk51Nh9aEaOJu2mOZIf36uDu6EDi3PVoIQGV5ef
iwSG1Rjny8COY3P4sI1WM2HKx4bpPYdEFlzA9RMOlhCAsLJssYqGxRbcZI8//9MfIrliDvjPOwqqL/xwD996P6rY9zGHWPNMNPf8UJl9+Cdm169G9YWOdapjB
8auShsJMc85YdekVWL7lQgroKHd68qMfRcAEu+lrX1GdSdmBKjQn0aOrU9lso5bK53uSLiyscNu10tAy66FganAQD9zwD6jM5ZBe2IeLbvoGWs5YofZQyfKXx
bpejl133omfXfth7P/Fz8NRLbXgb0nGNe26GhGST5MzFmEYll2oCl+sd2IZCcWtTKxd6rokwdYVpyK9fB1z1KnIrD0NDt1WiNGB738X3kxJVapiWVmR5pCurc
2iSaIkmNJ0Hr+9+WYkMu0YfHI7Dv9+J+766Eew8vSNiFP4WGsGBanhh6bw1K3fRjSdwfSel5FikTT67At4+t9vgVssojA0Rp6VwOyhfjx9262qABrfw1KaJW1
5YprXvsVcEG1sT5eCji40fXSURVyAvTd9TSmv6nTVifQx/uwzmHiU7kb3Clu+GC27MsY247p07+SihN0m/Kgc6EXRIjmMgDvCF9mcsXJxDgniZSnN3xFLIcc6
Yormd1mhCX2QpWc7SteolNUpNUQkIUvJpDkUrsrfqy1L8ZjaFSTrJKLsCbvz6BqxaBwdBReWbJmF3kTa2NYRVYFGHEYKqqFKFXtzMg6uUhaJyzZyQ/d/FdUm8
LwmAuYwO/vhQBU+m+ddmy+NpBKNWpIzF7EdRSxrOygMMl6LruUw2tQXOTy1akNFk/XtU/V70H3g6YyNNk5GtOIp/DYvlKp9LoJLWuIl2fADfJ/X71PQ8Jo2Vz
bv620OAFI9jtIqCQ7tnfC/JxhNT4dShds4UKvB66s1ftPnRqOh/l13hDDqWGhxqUgTsIV1Fzg5Y7TEpKsK+B/w+sdqUWuqv1CxUN8K/MqHLMnhj/g/J/4/juD
ky9VSg0kh/zQj322897Pao/8nwAC+AZicLeuzngAAAABJRU5ErkJggg==);
background-repeat: no-repeat;
background-position: top left;
height: 64px;
}
#header h1, #header h2 {margin: 0}
#header h2 {
color: #888;
font-weight: normal;
font-size: 16px;
}


#about h3 {
```

```
margin: 0;
margin-bottom: 10px;
font-size: 14px;
}

#about-content {
background-color: #ffd;
border: 1px solid #fc0;
margin-left: -55px;
margin-right: -10px;
}
#about-content table {
margin-top: 10px;
margin-bottom: 10px;
font-size: 11px;
border-collapse: collapse;
}
#about-content td {
padding: 10px;
padding-top: 3px;
padding-bottom: 3px;
}
#about-content td.name {color: #555}
#about-content td.value {color: #000}

#about-content ul {
padding: 0;
list-style-type: none;
}

#about-content.failure {
background-color: #fcc;
border: 1px solid #f00;
}
#about-content.failure p {
margin: 0;
padding: 10px;
}


#getting-started {
border-top: 1px solid #ccc;
margin-top: 25px;
padding-top: 15px;
}
#getting-started h1 {
margin: 0;
font-size: 20px;
}
#getting-started h2 {
margin: 0;
font-size: 14px;
font-weight: normal;
color: #333;
margin-bottom: 25px;
}
#getting-started ol {
margin-left: 0;
padding-left: 0;
}
#getting-started li {
font-size: 18px;
color: #888;
margin-bottom: 25px;
}
#getting-started li h2 {
margin: 0;
font-weight: normal;
font-size: 18px;
color: #333;
}
#getting-started li p {
color: #555;
font-size: 13px;
}


#sidebar ul {
margin-left: 0;
padding-left: 0;
}
#sidebar ul h3 {
margin-top: 25px;
font-size: 16px;
padding-bottom: 10px;
border-bottom: 1px solid #ccc;
}
#sidebar li {
```

```
list-style-type: none;
}
#sidebar ul.links li {
margin-bottom: 5px;
}

.filename {
font-style: italic;
}
</style>
<script>
function about() {
var info = document.getElementById('about-content'),
xhr;

if (info.innerHTML === '') {
xhr = new XMLHttpRequest();
xhr.open("GET", "/rails/info/properties", false);
xhr.setRequestHeader("X-Requested-With", "XMLHttpRequest");
xhr.send("");
info.innerHTML = xhr.responseText;
}

info.style.display = info.style.display === 'none' ? 'block' : 'none';
}
</script>
</head>
<body>
<div id="page">
<div id="sidebar">
<ul id="sidebar-items">
<li>
<h3>Browse the documentation</h3>
<ul class="links">
<li><a href="http://guides.rubyonrails.org/">Rails Guides</a></li>
<li><a href="http://api.rubyonrails.org/">Rails API</a></li>
<li><a href="http://www.ruby-doc.org/core/">Ruby core</a></li>
<li><a href="http://www.ruby-doc.org/stdlib/">Ruby standard library</a></li>
</ul>
</li>
</ul>
</div>

<div id="content">
<div id="header">
<h1>Welcome aboard</h1>
<h2>You&rsquo;re riding Ruby on Rails!</h2>
</div>

<div id="about">
<h3><a href="/rails/info/properties" onclick="about(); return false">About your application&rsquo;s environment</a></h3>
<div id="about-content" style="display: none"></div>
</div>

<div id="getting-started">
<h1>Getting started</h1>
<h2>Here&rsquo;s how to get rolling:</h2>

<ol>
<li>
<h2>Use <code>rails generate</code> to create your models and controllers</h2>
<p>To see all available options, run it without parameters.</p>
</li>

<li>
<h2>Set up a root route to replace this page</h2>
<p>You're seeing this page because you're running in development mode and you haven't set a root route yet.</p>
<p>Routes are set up in <span class="filename">config/routes.rb</span>.</p>
</li>

<li>
<h2>Configure your database</h2>
<p>If you're not using SQLite (the default), edit <span class="filename">config/database.yml</span> with your username
and password.</p>
</li>
</ol>
</div>
</div>

<div id="footer"> </div>
</div>
</body>
</html>
```

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/4848/www

```
Response Code : HTTP/1.1 200 OK

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

X-Powered-By: Servlet/3.1 JSP/2.3 (GlassFish Server Open Source Edition 4.0 Java/Oracle Corporation/1.8)
Server: GlassFish Server Open Source Edition 4.0
Content-Type: text/html;charset=UTF-8
Date: Wed, 11 Feb 2026 12:09:32 GMT
Transfer-Encoding: chunked

Response Body :


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
<head>
<title>Login</title>
<script type="text/javascript">
<!-- FIXME: add code to ensure we're the top-most frame -->
if (document.getElementById('layout-doc') != null) {
// Just refresh the page... login will take over
window.location = window.location;
}
</script>
<style type="text/css">
/* clickjacking defense */
body { display : none; }
</style>
<link rel="stylesheet" type="text/css" href="/theme/com/sun/webui/jsf/suntheme/css/css_master.css" />
<script type="text/javascript">
djConfig={
"isDebug": false,
"debugAtAllCosts": false,
"parseWidgets": false
};
</script>
<script type="text/javascript" src="/theme/META-INF/dojo/dojo.js"></script>
<script type="text/javascript" src="/theme/META-INF/json/json.js"></script>
<script type="text/javascript" src="/theme/META-INF/prototype/prototype.js"></script>
<script type="text/javascript" src="/theme/META-INF/com_sun_faces_ajax.js"></script>
<script type="text/javascript">
dojo.hostenv.setModulePrefix("webui.suntheme", "/theme/com/sun/webui/jsf/suntheme/javascript");
dojo.require('webui.suntheme.*');
</script>
<link id="sun_link5" rel="stylesheet" type="text/css" href="/resource/css/css_ns6up.css" />

</head>
```

```
<body id="body3" class="LogBdy" focus="loginform.j_username" style="background-color: #FFFFFF;">
<div id="header"class="LogTopBnd" style="background: url('/theme/com/sun/webui/jsf/suntheme/images/login/gradlogtop.jpg')
repeat-x; height: 30px;"></div>
<div class="middle" style="background-image:
url(/theme/com/sun/webui/jsf/suntheme/images/login/gradlogsides.jpg);background-repeat:repeat-x;background-position:left
top; background-color: #D4DCE1;">
<div class="plugincontent" style="width1: 1px; visibility: visible;">

<div style="height: 435px;background-image: url(/resource/community-theme/images/login-backimage-open.png);
background-repeat:no-repeat;background-position:left top; width: 720px; margin: auto;">
<div style="width: 460px; padding-top: 160px; margin-left: 310px;">
<img id="sun_image11" src="/resource/community-theme/images/login-product_name_open.png" alt="GlassFish Server Open
Source Edition" height="42" width="329" border="0" />
<form method="POST" class="form" name="loginform" action="j_security_check">
<table role="presentation">
<tr>
<td><label for="Login.username" style="font-weight: bold;">User Name:</label></td>
<td><input type="text" name="j_username" id="Login.username" tabindex="1" value=""></td>
</tr>
<tr>
<td><label for="Login.password" style="font-weight: bold;">Password:</label>
<td><input type="password" name="j_password" id="Login.password" tabindex="2">
<tr>
<td colspan="2" align="center">
<input type="submit" class="Btn1"
value="Login"
title="Log In to GlassFish Administration Console" tabindex="3"
onmouseover="javascript: if (this.disabled==0) this.className='Btn1Hov'"
onmouseout="javascript: if (this.disabled==0) this.className='Btn1'"
onblur="javascript: if (this.disabled==0) this.className='Btn1'"
onfocus="javascript: if (this.disabled==0) this.className='Btn1Hov'"
name="loginButton" id="loginButton">
<input type="hidden" name="loginButton.DisabledHiddenField" value="true" />
</td>
</tr>
</table>
</form>
</div>
</div>

<script type="text/javascript">
if (false) {
//submitAndDisable(document.getElementById('loginButton'), 'Login');
document.getElementById('loginButton').form.submit();
//document.getElementById('loginButton').form.autocomplete="off";
}
</script>
</div>
</div>
<div class="footer"
style="background-image: url(/theme/com/sun/webui/jsf/suntheme/images/login/gradlogbot.jpg);background-repeat:repeat-
x;background-position:left top; color: #FFFFFF; background-color: #4A5C68">
<div id="copyright" style="width: 720px; margin-left: auto; margin-right: auto; padding: 5px;">
<span>Copyright © 2005, 2013, Oracle and/or its affiliates. All rights reserved. Oracle and Java are registered
trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.</span>
</div>
</div>
<script src="/resource/js/cj.js"></script>
</body>
</html>
```

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/5985/www

```
Response Code : HTTP/1.1 404 Not Found

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

Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Wed, 11 Feb 2026 12:09:32 GMT
Connection: close
Content-Length: 315

Response Body :
```

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/8022/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 : no
Options allowed : GET, HEAD, POST, PUT, DELETE, OPTIONS
Headers :

Server: Apache-Coyote/1.1
Accept-Ranges: bytes
ETag: W/"107-1444224756000"
Last-Modified: Wed, 07 Oct 2015 13:32:36 GMT
Content-Type: text/html;charset=UTF-8
Content-Length: 107
Date: Wed, 11 Feb 2026 12:09:32 GMT

Response Body :
```

```
<!-- $Id$ -->
<html>
<head>
<META HTTP-EQUIV=Refresh CONTENT="0; URL=./configurations.do">
</head>
</html>
```

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/8080/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 : no
Options allowed : GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
Headers :

X-Powered-By: Servlet/3.1 JSP/2.3 (GlassFish Server Open Source Edition 4.0 Java/Oracle Corporation/1.8)
Server: GlassFish Server Open Source Edition 4.0
Accept-Ranges: bytes
ETag: W/"4626-1368596036000"
Last-Modified: Wed, 15 May 2013 05:33:56 GMT
Content-Type: text/html
Date: Wed, 11 Feb 2026 12:09:32 GMT
Content-Length: 4626

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html lang="en">
<!--
DO NOT ALTER OR REMOVE COPYRIGHT NOTICES OR THIS HEADER.

Copyright (c) 2010, 2013 Oracle and/or its affiliates. All rights reserved.

Use is subject to License Terms
-->
<head>
<style type="text/css">
body{margin-top:0}
body,td,p,div,span,a,ul,ul li, ol, ol li, ol li b, dl,h1,h2,h3,h4,h5,h6,li {font-family:geneva,helvetica,arial,"lucida
sans",sans-serif; font-size:10pt}
h1 {font-size:18pt}
h2 {font-size:14pt}
h3 {font-size:12pt}
code,kbd,tt,pre {font-family:monaco,courier,"courier new"; font-size:10pt;}
li {padding-bottom: 8px}
p.copy, p.copy a {font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:8pt}
p.copy {text-align: center}
table.grey1,tr.grey1,td.grey1{background:#f1f1f1}
```

```
th {color:#ffffff; font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:12pt}
td.insidehead {font-weight:bold; background:white; text-align: left;}
a {text-decoration:none; color:#3E6B8A}
a:visited{color:#917E9C}
a:hover {text-decoration:underline}
</style>
<title>GlassFish Server - Server Running</title>
</head>
<body bgcolor="#ffffff" text="#000000" link="#594fbf" vlink="#1005fb" alink="#333366"><br> <table width="100%" border="0"
cellspacing="0" cellpadding="3">
<tbody>
<tr><td align="right" valign="top"> <a href="http://www.oracle.com">oracle.com</a> </td></tr>
<tr><td align="left" valign="top" bgcolor="#587993"> <font color="#ffffff"> <b>GlassFish Server</b></font> </td>
</tr>
</tbody>
</table>
<h1>Your server is now running</h1>
<p>To replace this page, overwrite the file <code>index.html</code> in the document root folder of this server. The
document root folder for this server is the <code>docroot</code> subdirectory of this server's domain directory.</p>
<p>To manage a server on the <b>local host</b> with the <b>default administration port</b>, <a
href="http://localhost:4848">go to the Administration Console</a>.</p>
<!--
<h2>Get Oracle GlassFish Server with Premier Support</h2>
<p>For production deployments, consider Oracle GlassFish Server with <a
href="http://www.oracle.com/support/premier/index.html">Oracle Premier Support for Software</a>. Premier Support helps
lower the total cost and risk of owning your Oracle solutions, improve the return from your IT investment, and optimize
the business value of your IT solutions. Benefits of Premier Support include product updates and enhancements, global
reach, lifetime support, ecosystem support, and proactive, automated support.</p>
-->
<h2>Install and update additional software components</h2>
<p>Use the <a href="http://wikis.oracle.com/display/IpsBestPractices/">Update Tool</a> to install and update additional
technologies and frameworks such as:</p>
<ul>
<li>OSGi HTTP Service</li>
<li>Generic Resource Adapter for JMS</li>
<li>OSGi Administration Console</li>
</ul>
<p>If you are using the web profile, you can also use Update Tool to obtain technologies that are included by default in
the full platform, such as:</p>
<ul>
<li>Enterprise Java Beans</li>
<li><a href="http://metro.java.net/">Metro</a></li>
<li><a href="http://jersey.java.net/">Jersey</a></li>
</ul>
<p>To improve the user experience and optimize offerings to users, Oracle collects data about <a
href="http://wikis.oracle.com/display/GlassFish/UsageMetrics">GlassFish Server usage</a> that is transmitted by the
Update Tool installer as part of the automatic update processes. No personally identifiable information is collected by
this process.</p>
<h2>Join the GlassFish community</h2>
<p>Visit the <a href="http://glassfish.java.net">GlassFish Community</a> page for information about how to join the
GlassFish community. The GlassFish community is developing an open source, production-quality, enterprise-class
application server that implements the newest features of the Java&trade; Platform, Enterprise Edition (Java EE) platform
and related enterprise technologies.</p>
<h2>Learn more about GlassFish Server</h2>
<p>For more information about GlassFish Server, samples, documentation, and additional resources, see <var>as-
install</var><code>/docs/about.html</code>, where <var>as-install</var> is the GlassFish Server installation directory.
</p>
<hr style="width: 80%; height: 2px;">
<p class="copy"><a href="http://www.oracle.com/corporate/">Company Info</a>   |   <a
href="http://www.oracle.com/corporate/contact/">Contact</a>   |  
Copyright &copy; 2010, 2013 Oracle Corporation   |   <a href="./copyright.html">Legal Notices</a></p>
</body></html>
```

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/8181/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
Headers :

X-Powered-By: Servlet/3.1 JSP/2.3 (GlassFish Server Open Source Edition 4.0 Java/Oracle Corporation/1.8)
Server: GlassFish Server Open Source Edition 4.0
Accept-Ranges: bytes
ETag: W/"4626-1368596036000"
Last-Modified: Wed, 15 May 2013 05:33:56 GMT
Content-Type: text/html
Date: Wed, 11 Feb 2026 12:09:40 GMT
Content-Length: 4626

Response Body :

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html lang="en">
<!--
DO NOT ALTER OR REMOVE COPYRIGHT NOTICES OR THIS HEADER.

Copyright (c) 2010, 2013 Oracle and/or its affiliates. All rights reserved.

Use is subject to License Terms
-->
<head>
<style type="text/css">
body{margin-top:0}
body,td,p,div,span,a,ul,ul li, ol, ol li, ol li b, dl,h1,h2,h3,h4,h5,h6,li {font-family:geneva,helvetica,arial,"lucida
sans",sans-serif; font-size:10pt}
h1 {font-size:18pt}
h2 {font-size:14pt}
h3 {font-size:12pt}
code,kbd,tt,pre {font-family:monaco,courier,"courier new"; font-size:10pt;}
li {padding-bottom: 8px}
p.copy, p.copy a {font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:8pt}
p.copy {text-align: center}
table.grey1,tr.grey1,td.grey1{background:#f1f1f1}
th {color:#ffffff; font-family:geneva,helvetica,arial,"lucida sans",sans-serif; font-size:12pt}
td.insidehead {font-weight:bold; background:white; text-align: left;}
a {text-decoration:none; color:#3E6B8A}
a:visited{color:#917E9C}
a:hover {text-decoration:underline}
</style>
<title>GlassFish Server - Server Running</title>
</head>
<body bgcolor="#ffffff" text="#000000" link="#594fbf" vlink="#1005fb" alink="#333366"><br> <table width="100%" border="0"
cellspacing="0" cellpadding="3">
<tbody>
<tr><td align="right" valign="top"> <a href="http://www.oracle.com">oracle.com</a> </td></tr>
<tr><td align="left" valign="top" bgcolor="#587993"> <font color="#ffffff"> <b>GlassFish Server</b></font> </td>
</tr>
</tbody>
</table>
<h1>Your server is now running</h1>
<p>To replace this page, overwrite the file <code>index.html</code> in the document root folder of this server. The
document root folder for this server is the <code>docroot</code> subdirectory of this server's domain directory.</p>
<p>To manage a server on the <b>local host</b> with the <b>default administration port</b>, <a
href="http://localhost:4848">go to the Administration Console</a>.</p>
<!--
<h2>Get Oracle GlassFish Server with Premier Support</h2>
<p>For production deployments, consider Oracle GlassFish Server with <a
href="http://www.oracle.com/support/premier/index.html">Oracle Premier Support for Software</a>. Premier Support helps
lower the total cost and risk of owning your Oracle solutions, improve the return from your IT investment, and optimize
the business value of your IT solutions. Benefits of Premier Support include product updates and enhancements, global
reach, lifetime support, ecosystem support, and proactive, automated support.</p>
-->
<h2>Install and update additional software components</h2>
<p>Use the <a href="http://wikis.oracle.com/display/IpsBestPractices/">Update Tool</a> to install and update additional
technologies and frameworks such as:</p>
```

```
<ul>
<li>OSGi HTTP Service</li>
<li>Generic Resource Adapter for JMS</li>
<li>OSGi Administration Console</li>
</ul>
<p>If you are using the web profile, you can also use Update Tool to obtain technologies that are included by default in
the full platform, such as:</p>
<ul>
<li>Enterprise Java Beans</li>
<li><a href="http://metro.java.net/">Metro</a></li>
<li><a href="http://jersey.java.net/">Jersey</a></li>
</ul>
<p>To improve the user experience and optimize offerings to users, Oracle collects data about <a
href="http://wikis.oracle.com/display/GlassFish/UsageMetrics">GlassFish Server usage</a> that is transmitted by the
Update Tool installer as part of the automatic update processes. No personally identifiable information is collected by
this process.</p>
<h2>Join the GlassFish community</h2>
<p>Visit the <a href="http://glassfish.java.net">GlassFish Community</a> page for information about how to join the
GlassFish community. The GlassFish community is developing an open source, production-quality, enterprise-class
application server that implements the newest features of the Java&trade; Platform, Enterprise Edition (Java EE) platform
and related enterprise technologies.</p>
<h2>Learn more about GlassFish Server</h2>
<p>For more information about GlassFish Server, samples, documentation, and additional resources, see <var>as-
install</var><code>/docs/about.html</code>, where <var>as-install</var> is the GlassFish Server installation directory.
</p>
<hr style="width: 80%; height: 2px;">
<p class="copy"><a href="http://www.oracle.com/corporate/">Company Info</a>   |   <a
href="http://www.oracle.com/corporate/contact/">Contact</a>   |  
Copyright &copy; 2010, 2013 Oracle Corporation   |   <a href="./copyright.html">Legal Notices</a></p>
</body></html>
```

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/8383/www

```
Response Code : HTTP/1.1 200 OK

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

Date: Wed, 11 Feb 2026 12:09:32 GMT
Server: Apache
Accept-Ranges: bytes
ETag: W/"107-1444224756000"
Last-Modified: Wed, 07 Oct 2015 13:32:36 GMT
Content-Length: 107
X-dc-header: yes
Keep-Alive: timeout=5, max=98
Connection: Keep-Alive
```

```
Content-Type: text/html;charset=UTF-8

Response Body :

<!-- $Id$ -->
<html>
<head>
<META HTTP-EQUIV=Refresh CONTENT="0; URL=./configurations.do">
</head>
</html>
```

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/8484/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 : no
Options allowed : (Not implemented)
Headers :

X-Content-Type-Options: nosniff
Expires: 0
Cache-Control: no-cache,no-store,must-revalidate
X-Hudson-Theme: default
Content-Type: text/html;charset=UTF-8
X-Hudson: 1.395
X-Jenkins: 1.637
X-Jenkins-Session: 7e9144e5
X-Hudson-CLI-Port: 49232
X-Jenkins-CLI-Port: 49232
X-Jenkins-CLI2-Port: 49232
X-Frame-Options: sameorigin
X-Instance-Identity:
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuvOkpN9k5rcq4zdeu1hU+P+MRQmEO+wvne7AUO2Swl9ejHofmOWkRjxAURGK4s6G+damK+gLG7VKQ
iicL3SNdLrjAbYuKYCQ3NdfRkfe1NziMlHdiPEHnuuXMy3VMJyBD5mPwL/VgRmaSs5QvsJTA71Xo2iFzldebwclFK/Y/JB4ct+IoJqMmaZWjCyRWQUTim5W2+
qJRFnRXzllJCB8Dm9dVZnMxTmchWBFOoy1MSluae4CQjmovVu+INTv8JSPwnsjyZyCQKXjMHvak0/Iyw4RvKjoaaJwg9GA5fhpMNlEoDnMF2vBFGkz0+mg2AJ
Rw2f/OQ3M85r1N/IcmDE35QIDAQAB
X-SSH-Endpoint: 192.168.122.168:49231
Content-Length: 10655
Server: Jetty(winstone-2.8)

Response Body :



<!DOCTYPE html><html><head resURL="/static/7e9144e5">
```

<meta http-equiv="X-UA-Compatible" content="IE=Edge" /><title>Dashboard [Jenkins]</title><link rel="stylesheet" href="/static/7e9144e5/css/style.css" type="text/css" /><link rel="stylesheet" href="/static/7e9144e5/css/color.css" type="text/css" /><link rel="stylesheet" href="/static/7e9144e5/css/responsive-grid.css" type="text/css" /><link rel="shortcut icon" href="/static/7e9144e5/favicon.ico" type="image/vnd.microsoft.icon" /><link color="black" rel="mask-icon" href="/images/mask-icon.svg" /><script>var isRunAsTest=false; var rootURL=""; var resURL="/static/7e9144e5";
</script><script src="/static/7e9144e5/scripts/prototype.js" type="text/javascript"></script><script src="/static/7e9144e5/scripts/behavior.js" type="text/javascript"></script><script src='/adjuncts/7e9144e5/org/kohsuke/stapler/bind.js' type='text/javascript'></script><script src="/static/7e9144e5/scripts/yui/yahoo/yahoo-min.js"></script><script src="/static/7e9144e5/scripts/yui/dom/dom-min.js">
</script><script src="/static/7e9144e5/scripts/yui/event/event-min.js"></script><script src="/static/7e9144e5/scripts/yui/animation/animation-min.js"></script><script src="/static/7e9144e5/scripts/yui/dragdrop/dragdrop-min.js"></script><script src="/static/7e9144e5/scripts/yui/container/container-min.js"></script><script src="/static/7e9144e5/scripts/yui/connection/connection-min.js"></script><script src="/static/7e9144e5/scripts/yui/datasource/datasource-min.js"></script><script src="/static/7e9144e5/scripts/yui/autocomplete/autocomplete-min.js"></script><script src="/static/7e9144e5/scripts/yui/menu/menu-min.js"></script><script src="/static/7e9144e5/scripts/yui/element/element-min.js"></script><script src="/static/7e9144e5/scripts/yui/button/button-min.js"></script><script src="/static/7e9144e5/scripts/yui/storage/storage-min.js"></script><script src="/static/7e9144e5/scripts/hudson-behavior.js" type="text/javascript"></script><script src="/static/7e9144e5/scripts/sortable.js" type="text/javascript">
</script><script>crumb.init("", "");</script><link rel="stylesheet" href="/static/7e9144e5/scripts/yui/container/assets/container.css" type="text/css" /><link rel="stylesheet" href="/static/7e9144e5/scripts/yui/assets/skins/sam/skin.css" type="text/css" /><link rel="stylesheet" href="/static/7e9144e5/scripts/yui/container/assets/skins/sam/container.css" type="text/css" /><link rel="stylesheet" href="/static/7e9144e5/scripts/yui/button/assets/skins/sam/button.css" type="text/css" /><link rel="stylesheet" href="/static/7e9144e5/scripts/yui/menu/assets/skins/sam/menu.css" type="text/css" /><link rel="search" href="/opensearch.xml" type="application/opensearchdescription+xml" title="Jenkins" /><meta name="ROBOTS" content="INDEX,NOFOLLOW" /><link rel="alternate" href="/rssAll" title="Jenkins:All (all builds)" type="application/rss+xml" /><link rel="alternate" href="/rssAll?flavor=rss20" title="Jenkins:All (all builds) (RSS 2.0)" type="application/rss+xml" /><link rel="alternate" href="/rssFailed" title="Jenkins:All (failed builds)" type="application/rss+xml" /><link rel="alternate" href="/rssFailed?flavor=rss20" title="Jenkins:All (failed builds) (RSS 2.0)" type="application/rss+xml" /><script src="/static/7e9144e5/scripts/yui/cookie/cookie-min.js"></script><script>
YAHOO.util.Cookie.set("screenResolution", screen.width+"x"+screen.height);
</script><script src="/static/7e9144e5/scripts/yui/cookie/cookie-min.js"></script><script src="/static/7e9144e5/scripts/msie.js" type="text/javascript"></script></head><body data-model-type="hudson.model.AllView" id="jenkins" class="yui-skin-sam jenkins-1.637" data-version="jenkins-1.637">Skip to content <form method="get" name="search" action="/search/" style="position:relative;" class="no-json"> <input name="q" placeholder="search" id="search-box" class="has-default-text" />
<script>createSearchBox("/search/");</script> </form> <tr id="top-nav"><td id="left-top-nav" colspan="2"><link rel='stylesheet' href='/adjuncts/7e9144e5/lib/layout/breadcrumbs.css' type='text/css' /><script src='/adjuncts/7e9144e5/lib/layout/breadcrumbs.js' type='text/javascript'></script> ENABLE AUTO REFRESH <ul id="breadcrumbs"><li class="item">Jenkins
<li href="/" class="children"> </td></tr> New Item People Build History Manage Jenkins Credentials Build Queue <table class="pane "><tr><td class="pane" colspan="2">No builds in the queue.</td></tr></table> <script defer="defer">refreshPart('buildQueue',"/ajaxBuildQueue");</script> Build Executor Status <table class="pane "><colgroup><col width="30" /><col width="200*" /><col width="24" />
</colgroup><tr></tr><tr><td class="pane" align="right" style="vertical-align: top">1</td><td class="pane">Idle</td><td class="pane"></td><td class="pane"></td></tr><tr><td class="pane" align="right" style="vertical-align: top">2</td><td class="pane">Idle</td><td class="pane"></td><td class="pane"></td></tr></table> <script defer="defer">refreshPart('executors',"/ajaxExecutors");</script> add description <h1>Welcome to Jenkins!</h1> Please create new jobs to get started. <footer> Page generated: Feb 11, 2026 4:09:32 AMREST APIJenkins ver. 1.637 <div id="l10n-

```
footer" style="display:none; float:left"><a href="#" onclick="return showTranslationDialog();"><img
src="/static/7e9144e5/plugin/translation/flags.png" />
Help us localize this page
</a></div><script>var footer = document.getElementById('l10n-footer');
var f = document.getElementById('footer');
f.insertBefore(footer,f.firstChild);
footer.style.display="block";

var translation={};
translation.bundles =
"kJMKUWtb85oUX6VHB3/y0YVwXSBeApwPENoWnmknEi9mioPLiQ0wyJBQRD3niNPPQzZkp3lQ593oKaiNpMAYOYccoN3L8dGwbpXBR9t8W4zphAHJNnv3M1cT
D0AQb55KoInvpS6JzgL0snAlMPdK+7ysTuQ219lGPVhg/Oez0GoAZHb0x3c/29enWMVkSU4xwtk1s5Nn/jKb3OD7rMnKv5QKAv/+D5+PT234Jb1OzUkYV8faZ
C+aV1ng4d55MW01n1+Shuul5Z5aRJjbJH/zPJqWSHO9qR0ZS+Kxlirm2Pm3a2sgxASfW7DkZTdtohawrPtDnWUOJplJv2h3c8ImC6gG9Z4Zp/AR4PmKz6jQm1
d7D6PLjMjB/mVURQtiwadJ5ZoBgX6mBQm2dPPBYP/CXOnld4npVHAvf60D0ArWV5j71lUBOH7fEs96oA5DBnZD1eATL51qcJ35436CNwqk9xBf/EDInGgWgVb
eqaKD+NSn0ieI3wlNZxlkrR72iavbcIJnTOM+8STJQ+XGgCM3OzLLzZhZvIOVqkRk66HFmo+XHnvFOuv3Gkx9FGaPCuOa";
translation.detectedLocale = "";

function showTranslationDialog() {
if(!translation.launchDialog)
loadScript("/static/7e9144e5/plugin/translation/dialog.js");
else
translation.launchDialog();
return false;
}</script></div></div></div></footer></body></html>
```

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/9200/elasticsearch

```
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 : no
Options allowed : (Not implemented)
Headers :

Access-Control-Allow-Origin: *
Content-Type: application/json; charset=UTF-8
Content-Length: 308

Response Body :

{
"status" : 200,
"name" : "Magician",
"version" : {
"number" : "1.1.1",
"build_hash" : "f1585f096d3f3985e73456debdc1a0745f512bbc",
"build_timestamp" : "2014-04-16T14:27:12Z",
"build_snapshot" : false,
"lucene_version" : "4.7"
```

```
},
"tagline" : "You Know, for Search"
}
```

56877 - KVM / QEMU Guest Detection (uncredentialed check) -

Synopsis

The remote host is a KVM / QEMU virtual machine.

Description

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

Solution

Ensure that the host's configuration agrees with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2011/11/21, Modified: 2019/11/22

Plugin Output

tcp/0

53513 - Link-Local Multicast Name Resolution (LLMNR) Detection -

Synopsis

The remote device supports LLMNR.

Description

The remote device answered to a Link-local Multicast Name Resolution (LLMNR) request. This protocol provides a name lookup service similar to NetBIOS or DNS. It is enabled by default on modern Windows versions.

See Also

http://www.nessus.org/u?51eae65d
http://technet.microsoft.com/en-us/library/bb878128.aspx

Solution

Make sure that use of this software conforms to your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information

Published: 2011/04/21, Modified: 2023/10/17

Plugin Output

udp/5355/llmnr

```
According to LLMNR, the name of the remote host is 'vagrant-2008R2'.
```

71216 - ManageEngine Endpoint Central Detection -

Synopsis

The remote web server hosts a desktop and mobile device management application.

Description

The remote web server hosts ManageEngine Endpoint Central, a Java-based desktop and mobile device management web application.

See Also

https://www.manageengine.com/products/desktop-central/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0644

Plugin Information

Published: 2013/12/04, Modified: 2026/01/05

Plugin Output

tcp/8022/www

```
URL : http://192.168.122.168:8022/
Version : 9
build : 91084
```

71216 - ManageEngine Endpoint Central Detection -

Synopsis

The remote web server hosts a desktop and mobile device management application.

Description

The remote web server hosts ManageEngine Endpoint Central, a Java-based desktop and mobile device management web application.

See Also

https://www.manageengine.com/products/desktop-central/

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0644

Plugin Information

Published: 2013/12/04, Modified: 2026/01/05

Plugin Output

tcp/8383/www

```
URL : https://192.168.122.168:8383/
Version : 9
build : 91084
```

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure -

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/10/17, Modified: 2021/09/20

Plugin Output

tcp/445/cifs

```
The remote Operating System is : Windows Server 2008 R2 Standard 7601 Service Pack 1
The remote native LAN manager is : Windows Server 2008 R2 Standard 6.1
The remote SMB Domain Name is : VAGRANT-2008R2
```

11011 - Microsoft Windows SMB Service Detection -

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/139/smb

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

11011 - Microsoft Windows SMB Service Detection -

Synopsis

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

Description

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

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/06/05, Modified: 2021/02/11

Plugin Output

tcp/445/cifs

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

100871 - Microsoft Windows SMB Versions Supported (remote check) -

Synopsis

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

Description

Nessus was able to obtain the version of SMB running on the remote host by sending an authentication request to port 139 or 445.

Note that this plugin is a remote check and does not work on agents.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2017/06/19, Modified: 2019/11/22

Plugin Output

tcp/445/cifs

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

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/135/epmap

```
Port 135/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/139/smb

```
Port 139/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/445/cifs

```
Port 445/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/1617

```
Port 1617/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/3000/www

```
Port 3000/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/3306/mysql

```
Port 3306/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/3389/msrdp

```
Port 3389/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/3700/giop

```
Port 3700/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/4848/www

```
Port 4848/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/5985/www

```
Port 5985/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/7676/imqbrokerd

```
Port 7676/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/8019

```
Port 8019/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/8022/www

```
Port 8022/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/8028

```
Port 8028/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/8032

```
Port 8032/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/8080/www

```
Port 8080/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/8181/www

```
Port 8181/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/8383/www

```
Port 8383/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/8443

```
Port 8443/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/8444

```
Port 8444/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/8484/www

```
Port 8484/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/9200/elasticsearch

```
Port 9200/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: 2025/10/29

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.11.2
Nessus build : 20042
Plugin feed version : 202601122337
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : es9-x86-64
Scan type : Normal
Scan name : My Basic Network Scan
Scan policy used : Basic Network Scan
Scanner IP : 192.168.122.1
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 53.489 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 : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2026/2/11 13:02 CET (UTC +01:00)
Scan duration : 1459 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 : Microsoft Windows 8.1
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : Microsoft Windows 7
Microsoft Windows Server 2008 R2
Confidence level : 70
Method : Misc
Type : general-purpose
Fingerprint : unknown

Remote operating system : Microsoft Windows XP Professional
Microsoft Windows Server 2008 R2
Microsoft Windows 10
Confidence level : 66
Method : RDP
Type : general-purpose
Fingerprint : RDP:000000000f00000010000100080001000900000001001000100010

Remote operating system : Microsoft Windows
Confidence level : 70
Method : HTTP
Type : general-purpose
Fingerprint : HTTP:Server: Microsoft-HTTPAPI/2.0


Remote operating system : Microsoft Windows
Confidence level : 70
Method : SinFP
Type : general-purpose
Fingerprint : SinFP:
P1:B11113:F0x12:W8192:O0204ffff:M1460:
P2:B11113:F0x12:W8192:O0204ffff010303080402080affffffff44454144:M1460:
P3:B11121:F0x04:W0:O0:M0
P4:191602_7_p=8019

Remote operating system : Windows 6.1
Confidence level : 70
Method : smb
Type : general-purpose
Fingerprint : unknown

Remote operating system : Microsoft Windows Server 2008 R2 Standard Service Pack 1
Confidence level : 99
Method : MSRPC
Type : general-purpose
Fingerprint : unknown
```

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 : Microsoft Windows Server 2008 R2 Standard Service Pack 1
Confidence level : 99
Method : MSRPC

The remote host is running Microsoft Windows Server 2008 R2 Standard Service Pack 1
```

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 SMB service.
```

10919 - Open Port Re-check -

Synopsis

Previously open ports are now closed.

Description

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

There are several possible reasons for this :

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

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

This might be an availability problem related to the following :

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

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

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

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

Solution

Steps to resolve this issue include :

- Increase checks_read_timeout and/or reduce max_checks.

- Disable any IPS during the Nessus scan

Risk Factor

None

References

XREF IAVB:0001-B-0509

Plugin Information

Published: 2002/03/19, Modified: 2023/06/20

Plugin Output

tcp/0

```
Port 8019 was detected as being open but is now closed
Port 135 was detected as being open but is now closed
Port 3306 was detected as being open but is now closed
Port 3389 was detected as being open but is now closed
Port 8181 was detected as being open but is now closed
Port 1617 was detected as being open but is now closed
Port 8383 was detected as being open but is now closed
Port 8022 was detected as being open but is now closed
Port 5985 was detected as being open but is now closed
Port 8032 was detected as being open but is now closed
Port 3700 was detected as being open but is now closed
Port 7676 was detected as being open but is now closed
Port 8443 was detected as being open but is now closed
Port 8080 was detected as being open but is now closed
Port 8444 was detected as being open but is now closed
```

```
Port 4848 was detected as being open but is now closed
Port 3000 was detected as being open but is now closed
Port 8028 was detected as being open but is now closed
Port 9200 was detected as being open but is now closed
Port 8484 was detected as being open but is now closed
```

55930 - Oracle GlassFish HTTP Server Version -

Synopsis

It was possible to obtain the version number of the remote Oracle GlassFish HTTP server.

Description

The remote host is running an Oracle GlassFish HTTP Server, a Java EE application server. It was possible to read the version number from the HTTP response headers.

See Also

http://www.nessus.org/u?85f4fd5a

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/08/16, Modified: 2022/10/12

Plugin Output

tcp/4848/www

```
URL : https://192.168.122.168:4848/
Version : 4.0
```

55930 - Oracle GlassFish HTTP Server Version -

Synopsis

It was possible to obtain the version number of the remote Oracle GlassFish HTTP server.

Description

The remote host is running an Oracle GlassFish HTTP Server, a Java EE application server. It was possible to read the version number from the HTTP response headers.

See Also

http://www.nessus.org/u?85f4fd5a

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/08/16, Modified: 2022/10/12

Plugin Output

tcp/8080/www

```
URL : http://192.168.122.168:8080/
Version : 4.0
```

55930 - Oracle GlassFish HTTP Server Version -

Synopsis

It was possible to obtain the version number of the remote Oracle GlassFish HTTP server.

Description

The remote host is running an Oracle GlassFish HTTP Server, a Java EE application server. It was possible to read the version number from the HTTP response headers.

See Also

http://www.nessus.org/u?85f4fd5a

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/08/16, Modified: 2022/10/12

Plugin Output

tcp/8181/www

```
URL : https://192.168.122.168:8181/
Version : 4.0
```

55929 - Oracle GlassFish Server Administration Console -

Synopsis

It was possible to access the administration console of the remote Oracle GlassFish application server.

Description

The remote host is running the Oracle GlassFish application server, and has the administration console listening on an external IP.

See Also

http://www.nessus.org/u?85f4fd5a

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/08/16, Modified: 2019/11/22

Plugin Output

tcp/4848/www

```
Oracle GlassFish Server Administration Console detected on port 4848.
```

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: 2025/12/15

Plugin Output

tcp/0

```
. You need to take the following 3 actions :


[ Elasticsearch ESA-2015-06 (119499) ]

+ Action to take : Users should upgrade to 1.6.1 or 1.7.0. Alternately, ensure that only trusted applications have access
to the transport protocol port.


[ Elasticsearch Transport Protocol Unspecified Remote Code Execution (105752) ]

+ Action to take : Users should upgrade to 1.6.1 or 1.7.0. Alternately, ensure that only trusted applications have access
to the transport protocol port


[ ManageEngine Desktop Central < 10 Build 10.0.533 Integer Overflow (139377) ]

+ Action to take : Upgrade to ManageEngine Desktop Central version 10 build 10.0.533 or later.

+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).
```

66173 - RDP Screenshot -

Synopsis

It is possible to take a screenshot of the remote login screen.

Description

This script attempts to connect to the remote host via RDP (Remote Desktop Protocol) and attempts to take a screenshot of the login screen.

While this is not a vulnerability by itself, some versions of Windows display the names of the users who can connect and which ones are connected already.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/04/22, Modified: 2025/09/29

Plugin Output

tcp/3389/msrdp

```
It was possible to gather the following screenshot of the remote login screen.
```

10940 - Remote Desktop Protocol Service Detection -

Synopsis

The remote host has an remote desktop protocol service enabled.

Description

The Remote Desktop Protocol allows a user to remotely obtain a graphical login (and therefore act as a local user on the remote host).

If an attacker gains a valid login and password, this service could be used to gain further access on the remote host. An attacker may also use this service to mount a dictionary attack against the remote host to try to log in remotely.

Note that RDP (the Remote Desktop Protocol) is vulnerable to Man-in-the-middle attacks, making it easy for attackers to steal the credentials of legitimate users by impersonating the Windows server.

Solution

Disable the service if you do not use it, and do not allow this service to run across the Internet.

Risk Factor

None

Plugin Information

Published: 2002/04/20, Modified: 2023/08/21

Plugin Output

tcp/3389/msrdp

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

Synopsis

The remote host supports the SMBv1 protocol.

Description

The remote host (Windows and/or Samba server) supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, most security and compliance agencies recommend that users disable SMBv1 per SMB best practices.

See Also

http://www.nessus.org/u?59bfc3ef
http://www.nessus.org/u?b9d9ebf9
http://www.nessus.org/u?8dcab5e4
http://www.nessus.org/u?234f8ef8
http://www.nessus.org/u?4c7e0cf3

Solution

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

Risk Factor

None

References

XREF IAVT:0001-T-0710

Plugin Information

Published: 2017/02/03, Modified: 2025/08/13

Plugin Output

tcp/445/cifs

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

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: 2026/01/12

Plugin Output

tcp/3000/www

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

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2026/01/12

Plugin Output

tcp/3700/giop

```
A GIOP-enabled service 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: 2026/01/12

Plugin Output

tcp/4848/www

```
A TLSv1.2 server answered on this port.
```

tcp/4848/www

```
A web server is running on this port through TLSv1.2.
```

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: 2026/01/12

Plugin Output

tcp/5985/www

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

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2026/01/12

Plugin Output

tcp/8022/www

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

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2026/01/12

Plugin Output

tcp/8080/www

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

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2026/01/12

Plugin Output

tcp/8181/www

```
A TLSv1.1 server answered on this port.
```

tcp/8181/www

```
A web server is running on this port through TLSv1.1.
```

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: 2026/01/12

Plugin Output

tcp/8383/www

```
A TLSv1.2 server answered on this port.
```

tcp/8383/www

```
A web server is running on this port through TLSv1.2.
```

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: 2026/01/12

Plugin Output

tcp/8443

```
A TLSv1 server answered 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: 2026/01/12

Plugin Output

tcp/8484/www

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

22964 - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/08/19, Modified: 2026/01/12

Plugin Output

tcp/9200/elasticsearch

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

17975 - Service Detection (GET request) -

Synopsis

The remote service could be identified.

Description

It was possible 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

References

XREF IAVT:0001-T-0935

Plugin Information

Published: 2005/04/06, Modified: 2021/10/27

Plugin Output

tcp/3306/mysql

```
A MySQL server seems to be running on this port but the Nessus scanner
IP has been blacklisted. Run 'mysqladmin flush-hosts' if you want
complete tests.
```

14773 - Service Detection: 3 ASCII Digit Code Responses -

Synopsis

This plugin performs service detection.

Description

This plugin is a complement of find_service1.nasl. It attempts to identify services that return 3 ASCII digits codes (ie: FTP, SMTP, NNTP, ...)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2004/09/17, Modified: 2025/12/16

Plugin Output

tcp/7676/imqbrokerd

```
A Message Queue broker is listening on this port.
```

278501 - Smartbedded Meteobridge Web Detection -

Synopsis

The web UI for Smartbedded Meteobridge was detected on the remote host.

Description

Smartbedded Meteobridge, a dedicated weather monitoring application, is running on the remote host.

Note: Basic HTTP Authentication credentials are required to obtain the version.

See Also

https://www.meteobridge.com/wiki/index.php?title=Meteobridge_VM
http://www.nessus.org/u?5ceb65be

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/12/12, Modified: 2026/01/05

Plugin Output

tcp/3000/www

```
URL : http://192.168.122.168:3000/cgi-bin/meteobridge
Version : unknown
Authenticated : False
```

278501 - Smartbedded Meteobridge Web Detection -

Synopsis

The web UI for Smartbedded Meteobridge was detected on the remote host.

Description

Smartbedded Meteobridge, a dedicated weather monitoring application, is running on the remote host.

Note: Basic HTTP Authentication credentials are required to obtain the version.

See Also

https://www.meteobridge.com/wiki/index.php?title=Meteobridge_VM
http://www.nessus.org/u?5ceb65be

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/12/12, Modified: 2026/01/05

Plugin Output

tcp/4848/www

```
URL : https://192.168.122.168:4848/cgi-bin/meteobridge
```

```
Version : unknown
Authenticated : False
```

278501 - Smartbedded Meteobridge Web Detection -

Synopsis

The web UI for Smartbedded Meteobridge was detected on the remote host.

Description

Smartbedded Meteobridge, a dedicated weather monitoring application, is running on the remote host.

Note: Basic HTTP Authentication credentials are required to obtain the version.

See Also

https://www.meteobridge.com/wiki/index.php?title=Meteobridge_VM
http://www.nessus.org/u?5ceb65be

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/12/12, Modified: 2026/01/05

Plugin Output

tcp/5985/www

```
URL : http://192.168.122.168:5985/cgi-bin/meteobridge
Version : unknown
Authenticated : False
```

278501 - Smartbedded Meteobridge Web Detection -

Synopsis

The web UI for Smartbedded Meteobridge was detected on the remote host.

Description

Smartbedded Meteobridge, a dedicated weather monitoring application, is running on the remote host.

Note: Basic HTTP Authentication credentials are required to obtain the version.

See Also

https://www.meteobridge.com/wiki/index.php?title=Meteobridge_VM
http://www.nessus.org/u?5ceb65be

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/12/12, Modified: 2026/01/05

Plugin Output

tcp/8022/www

```
URL : http://192.168.122.168:8022/cgi-bin/meteobridge
Version : unknown
Authenticated : False
```

278501 - Smartbedded Meteobridge Web Detection -

Synopsis

The web UI for Smartbedded Meteobridge was detected on the remote host.

Description

Smartbedded Meteobridge, a dedicated weather monitoring application, is running on the remote host.

Note: Basic HTTP Authentication credentials are required to obtain the version.

See Also

https://www.meteobridge.com/wiki/index.php?title=Meteobridge_VM
http://www.nessus.org/u?5ceb65be

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/12/12, Modified: 2026/01/05

Plugin Output

tcp/8080/www

```
URL : http://192.168.122.168:8080/cgi-bin/meteobridge
Version : unknown
Authenticated : False
```

278501 - Smartbedded Meteobridge Web Detection -

Synopsis

The web UI for Smartbedded Meteobridge was detected on the remote host.

Description

Smartbedded Meteobridge, a dedicated weather monitoring application, is running on the remote host.

Note: Basic HTTP Authentication credentials are required to obtain the version.

See Also

https://www.meteobridge.com/wiki/index.php?title=Meteobridge_VM
http://www.nessus.org/u?5ceb65be

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/12/12, Modified: 2026/01/05

Plugin Output

tcp/8181/www

```
URL : https://192.168.122.168:8181/cgi-bin/meteobridge
Version : unknown
Authenticated : False
```

278501 - Smartbedded Meteobridge Web Detection -

Synopsis

The web UI for Smartbedded Meteobridge was detected on the remote host.

Description

Smartbedded Meteobridge, a dedicated weather monitoring application, is running on the remote host.

Note: Basic HTTP Authentication credentials are required to obtain the version.

See Also

https://www.meteobridge.com/wiki/index.php?title=Meteobridge_VM
http://www.nessus.org/u?5ceb65be

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/12/12, Modified: 2026/01/05

Plugin Output

tcp/8383/www

```
URL : https://192.168.122.168:8383/cgi-bin/meteobridge
Version : unknown
Authenticated : False
```

278501 - Smartbedded Meteobridge Web Detection -

Synopsis

The web UI for Smartbedded Meteobridge was detected on the remote host.

Description

Smartbedded Meteobridge, a dedicated weather monitoring application, is running on the remote host.

Note: Basic HTTP Authentication credentials are required to obtain the version.

See Also

https://www.meteobridge.com/wiki/index.php?title=Meteobridge_VM
http://www.nessus.org/u?5ceb65be

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/12/12, Modified: 2026/01/05

Plugin Output

tcp/8484/www

```
URL : http://192.168.122.168:8484/cgi-bin/meteobridge
Version : unknown
Authenticated : False
```

278501 - Smartbedded Meteobridge Web Detection -

Synopsis

The web UI for Smartbedded Meteobridge was detected on the remote host.

Description

Smartbedded Meteobridge, a dedicated weather monitoring application, is running on the remote host.

Note: Basic HTTP Authentication credentials are required to obtain the version.

See Also

https://www.meteobridge.com/wiki/index.php?title=Meteobridge_VM
http://www.nessus.org/u?5ceb65be

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2025/12/12, Modified: 2026/01/05

Plugin Output

tcp/9200/elasticsearch

```
URL : http://192.168.122.168:9200/cgi-bin/meteobridge
Version : unknown
Authenticated : False
```

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

```
SMB was detected on port 445 but no credentials were provided.
SMB local checks were not enabled.
```

64814 - Terminal Services Use SSL/TLS -

Synopsis

The remote Terminal Services use SSL/TLS.

Description

The remote Terminal Services is configured to use SSL/TLS.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2013/02/22, Modified: 2023/07/10

Plugin Output

tcp/3389/msrdp

```
Subject Name:

Common Name: vagrant-2008R2
```

```
Issuer Name:

Common Name: vagrant-2008R2

Serial Number: 12 61 C3 4C 22 0B 4A B8 47 7F FE D6 5B 58 9F 30

Version: 3

Signature Algorithm: SHA-1 With RSA Encryption

Not Valid Before: Feb 10 19:09:42 2026 GMT
Not Valid After: Aug 12 19:09:42 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 B7 38 27 CC 1D DE E9 F7 D1 34 8C ED F0 D3 46 87 1E 37 82
F3 83 AC B2 3C 6A 12 D1 D6 76 FE DF 1F 5B C1 77 39 C0 F7 8D
D1 B9 23 AA 44 F5 ED 08 4D A8 69 03 96 CB BD 02 FC 29 83 4D
29 CD 89 79 94 0C B6 5F 3B 21 60 7B D6 7D 60 25 1F C7 F0 C8
82 7D FA EF D1 AA 61 B6 E9 F7 CA 11 CA 0E AA 4C 6D D9 6E 6C
D7 20 03 F2 59 62 C3 E0 66 92 51 4B 55 04 BC 23 CE 7F 3B 56
6F 52 11 FD E6 54 D2 7A BE EF D8 2C F7 E1 ED 85 E5 88 AB 81
FA 3E 46 69 83 89 0E 56 D1 10 44 67 E7 34 3A BB 15 CD CC B5
2F F8 73 EC 92 20 10 AF 97 43 AD D1 21 A0 7F 13 76 89 33 55
C9 32 25 B2 0C 11 2F A2 5C 58 70 E3 5A AA F0 E4 CE 0F 11 B0
57 40 B3 85 05 7B 4C 4F A3 20 87 AE A7 14 81 CF 96 D3 4A F4
1B B4 01 19 F8 6B 05 26 9A 10 41 22 2F BD 6E 65 17 3A A8 63
48 64 06 D4 AA 68 77 79 8D A7 3C B1 14 6A D2 B1 91
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 B6 7F AD 40 8F 9B 64 F3 03 24 1D 77 67 12 8B 5D F9 44 20
E0 EA 67 DA 97 6A B2 95 28 B0 9F 6F D8 B0 9E D0 30 D6 1D 23
D6 C1 6A 5C 1A 1F CE 6E D4 0F EC 39 13 66 12 34 B5 D7 81 3A
37 96 2F 62 0A D5 9C 79 91 8A 35 50 C6 26 39 EA AF 37 0D 93
59 54 17 2B 7B 39 D9 FC 0E 59 EB 9D D6 31 90 66 2E 20 56 0A
19 96 9F B5 9C 7F B4 77 F5 F2 96 E8 EC B9 13 63 3F CC C2 E5
1F 76 51 BE C2 52 CE 98 10 4E 04 90 30 6E C3 3F AF 67 A0 A6
9F E7 78 98 DA 20 C5 AF FF B1 D9 9A 3C D9 9A 1F 16 BA 6A 4A
B6 C4 AB F9 82 C5 F0 D5 30 77 95 49 AA 2F 7E E9 40 E5 F3 80
E9 67 C9 4D EE 53 F4 AB F4 94 1C 37 08 35 CD 21 37 7B 86 15
A0 40 D2 44 39 4E 29 27 98 6C D5 B4 5F 54 DF 02 89 62 C0 D6
3C B5 E5 76 68 64 C3 F2 D9 A2 C4 6C F3 B2 E1 75 4E 6A D0 A7
39 13 02 43 D5 37 E4 1F 8C DF 94 BC FA E1 F7 B0 BB

Extension: Extended Key Usage(2.5.29.37)
Critical: 0
Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1)


Extension: Key Usage(2.5.29.15)
Critical: 0
Key Usage: Key Encipherment, Data Encipherment
```

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 192.168.122.1 to 192.168.122.168 :
192.168.122.1

ttl was greater than 50 - Completing Traceroute.

?

Hop Count: 1

An error was detected along the way.
```

11154 - Unknown Service Detection: Banner Retrieval -

Synopsis

There is an unknown service running on the remote host.

Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2022/07/26

Plugin Output

tcp/8032

```
If you know what this service is and think the banner could be used to
identify it, please send a description of the service along with the
following output to svc-signatures@nessus.org :

Port : 8032
Type : get_http
Banner :
0x00: 49 6E 76 61 6C 69 64 20 46 54 20 47 57 41 44 44 Invalid FT GWADD
0x10: 52 20 2F 20 53 54 41 52 54 20 70 72 6F 74 6F 63 R / START protoc
0x20: 6F 6C 0A ol.
```

11154 - Unknown Service Detection: Banner Retrieval -

Synopsis

There is an unknown service running on the remote host.

Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2022/07/26

Plugin Output

tcp/8443

```
If you know what this service is and think the banner could be used to
identify it, please send a description of the service along with the
following output to svc-signatures@nessus.org :

Port : 8443
Type : get_http
Banner :
0x00: 49 6E 76 61 6C 69 64 20 47 57 41 44 44 52 20 2F Invalid GWADDR /
0x10: 20 53 54 41 52 54 20 70 72 6F 74 6F 63 6F 6C 0A START protocol.
0x20:
```

11154 - Unknown Service Detection: Banner Retrieval -

Synopsis

There is an unknown service running on the remote host.

Description

Nessus was unable to identify a service on the remote host even though it returned a banner of some type.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2002/11/18, Modified: 2022/07/26

Plugin Output

tcp/8444

```
If you know what this service is and think the banner could be used to
identify it, please send a description of the service along with the
following output to svc-signatures@nessus.org :

Port : 8444
Type : get_http
Banner :
0x00: 49 6E 76 61 6C 69 64 20 47 57 41 44 44 52 20 2F Invalid GWADDR /
0x10: 20 53 54 41 52 54 20 70 72 6F 74 6F 63 6F 6C 0A START protocol.
0x20:
```

33139 - WS-Management Server Detection -

Synopsis

The remote web server is used for remote management.

Description

The remote web server supports the Web Services for Management (WS-Management) specification, a general web services protocol based on SOAP for managing systems, applications, and other such entities.

See Also

https://www.dmtf.org/standards/ws-man
https://en.wikipedia.org/wiki/WS-Management

Solution

Limit incoming traffic to this port if desired.

Risk Factor

None

Plugin Information

Published: 2008/06/11, Modified: 2021/05/19

Plugin Output

tcp/5985/www

```
Here is some information about the WS-Management Server :

Product Vendor : Microsoft Corporation
Product Version : OS: 0.0.0 SP: 0.0 Stack: 3.0
```

10386 - Web Server No 404 Error Code Check -

Synopsis

The remote web server does not return 404 error codes.

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2000/04/28, Modified: 2022/06/17

Plugin Output

tcp/4848/www

```
The following string will be used :
TYPE="password"
```

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/8484/www

```
Contents of robots.txt :

# we don't want robots to click "build" links
User-agent: *
Disallow: /
```

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure -

Synopsis

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

Description

The remote host is listening on UDP port 137 or TCP port 445, and replies to NetBIOS nbtscan or SMB requests.

Note that this plugin gathers information to be used in other plugins, but does not itself generate a report.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/10/12, Modified: 2021/02/10

Plugin Output

udp/137/netbios-ns

```
The following 3 NetBIOS names have been gathered :

VAGRANT-2008R2 = Computer name
WORKGROUP = Workgroup / Domain name
VAGRANT-2008R2 = File Server Service

The remote host has the following MAC address on its adapter :

52:54:00:64:7e:b3
```