Tenable Vulnerability Management Report

Tenable Vulnerability Management

Thu, 05 Feb 2026 06:54:48 UTC

Table Of Contents

Vulnerabilities By Host

10.1.0.141

Scan Information

Start time:	2026/02/05 06:30
End time:	2026/02/05 06:54

Host Information

Netbios Name:	notengo
OS:	Microsoft Windows 11 Pro Build 26200

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	4	0	94	99

Results Details

/

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:

Publication date: 1999/10/12, Modification date: 2021/02/10

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```
The following 2 NetBIOS names have been gathered :

 notengo           = Computer name
 notengo           = Workgroup / Domain name
```

16193 - Antivirus Software Check

Synopsis

An antivirus application is installed on the remote host.

Description

An antivirus application is installed on the remote host, and its engine and virus definitions are up to date.

See Also

http://www.nessus.org/u?3ed73b52

https://www.tenable.com/blog/auditing-anti-virus-products-with-nessus

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2005/01/18, Modification date: 2025/05/27

Ports

10.1.0.141 (TCP/445) Vulnerability State: Resurfaced

```
Forefront_Endpoint_Protection :

A Microsoft anti-malware product is installed on the remote host :

  Product name                  : Windows Defender
  Path                          : C:\ProgramData\Microsoft\Windows Defender\Platform
\4.18.25110.6-0\
  Version                       : 4.18.25110.6
  Engine version                : 1.1.25110.1
  Antivirus signature version   : 1.443.1006.0
  Antispyware signature version : 1.443.1006.0
```

34097 - BIOS Info (SMB)

Synopsis

BIOS info could be read.

Description

It is possible to get information about the BIOS via the host's SMB interface.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2008/09/08, Modification date: 2024/06/11

Ports

10.1.0.141 (TCP/0) Vulnerability State: Resurfaced

```
  Version      :
  Release date :
  Secure boot  : disabled
```

42898 - SMB Registry : Stop the Registry Service after the scan (WMI)

Synopsis

The registry service was stopped after the scan.

Description

To perform a full credentialed scan, Nessus needs the ability to connect to the remote registry service (RemoteRegistry). If the service is down and if Nessus automatically enabled the registry for the duration of the scan, this plugins will stop it afterwards.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2009/11/25, Modification date: 2026/01/20

Ports

10.1.0.141 (TCP/0) Vulnerability State: Active

```
The registry service was successfully stopped after the scan.
```

57033 - Microsoft Patch Bulletin Feasibility Check

Synopsis

Nessus is able to check for Microsoft patch bulletins.

Description

Using credentials supplied in the scan policy, Nessus is able to collect information about the software and patches installed on the remote Windows host and will use that information to check for missing Microsoft security updates. Note that this plugin is purely informational.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2011/12/06, Modification date: 2021/07/12

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```
Nessus is able to test for missing patches using :
  Nessus
```

58452 - Microsoft Windows Startup Software Enumeration

Synopsis

It is possible to enumerate startup software.

Description

This plugin lists software that is configured to run on system startup by crawling the registry entries in :
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersi on\Run

Solution

Review the list of applications and remove any that are not compliant with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2012/03/23, Modification date: 2022/02/01

Ports

10.1.0.141 (TCP/445) Vulnerability State: Resurfaced

```
The following startup item was found :

  SecurityHealth - %windir%\system32\SecurityHealthSystray.exe
```

92428 - Recent File History

Synopsis

Nessus was able to enumerate recently opened files on the remote host.

Description

Nessus was able to gather evidence of files opened by file type from the remote host.

See Also

https://www.4n6k.com/2014/02/forensics-quickie-pinpointing-recent.html

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/11/15

Ports

10.1.0.141 (TCP/0) Vulnerability State: Resurfaced

```
C:\\Users\Notengo\AppData\Roaming\Microsoft\Windows\Recent\System32.lnk

Recent files found in registry and appdata attached.
```

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:

Publication date: 2017/06/19, Modification date: 2019/11/22

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

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

160301 - Link-Local Multicast Name Resolution (LLMNR) Service Detection

Synopsis

Verify status of the LLMNR service on the remote host.

Description

The Link-Local Multicast Name Resolution (LLMNR) service allows both IPv4 and IPv6 hosts to perform name resolution for hosts on the same local link

See Also

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:

Publication date: 2022/04/28, Modification date: 2022/12/29

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```
LLMNR Key SOFTWARE\Policies\Microsoft\Windows NT\DNSClient\EnableMulticast not found.
```

160576 - Windows Services Registry ACL

Synopsis

Checks Windows Registry for Service ACLs

Description

Checks Windows Registry for Service ACLs.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2022/05/05, Modification date: 2024/01/15

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```
Verbosity must be set to 'Report as much information as possible' for this plugin to produce
 output.
```

162174 - Windows Always Installed Elevated Status

Synopsis

Windows AlwaysInstallElevated policy status was found on the remote Windows host

Description

Windows AlwaysInstallElevated policy status was found on the remote Windows host.
You can use the AlwaysInstallElevated policy to install a Windows Installer package with elevated (system) privileges This option is equivalent to granting full administrative rights, which can pose a massive security risk. Microsoft strongly discourages the use of this setting.

Solution

If enabled, disable AlwaysInstallElevated policy per your corporate security guidelines.

Risk Factor

None

Plugin Information:

Publication date: 2022/06/14, Modification date: 2022/06/14

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```
AlwaysInstallElevated policy is not enabled under HKEY_LOCAL_MACHINE.
AlwaysInstallElevated policy is not enabled under HKEY_USERS
 user:S-1-5-21-1658136452-1347933459-2279167012-500
```

10396 - Microsoft Windows SMB Shares Access

Synopsis

It is possible to access a network share.

Description

The remote has one or more Windows shares that can be accessed through the network with the given credentials.
Depending on the share rights, it may allow an attacker to read / write confidential data.

Solution

To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing' tab, and click on 'permissions'.

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2021/10/04

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```

The following shares can be accessed as Notengo :

- ADMIN$  - (readable,writable)
  + Content of this share :
..
appcompat
apppatch
AppReadiness
assembly
bcastdvr
bfsvc.exe
Boot
bootstat.dat
Branding
BrowserCore
```

```
CbsTemp
command_results.log
Containers
CSC
Cursors
debug
diagnostics
DiagTrack
DigitalLocker
Downloaded Program Files
DtcInstall.log
ELAMBKUP
en-US
explorer.exe
Fonts
GameBarPresenceWriter
Globalization
Help
HelpPane.exe
hh.exe
IdentityCRL
IME
ImmersiveControlPanel
InboxApps
INF
InputMethod
Installer
L2Schemas
LanguageOverlayCache
LiveKernelReports
Logs
lsasetup.log
Media
mib.bin
Microsoft
Microsoft.NET
Migration
ModemLogs
notepad.exe
OCR
OEM
Offline Web Pages
Panther
Performance
PFRO.log
PLA
PolicyDefinitions
Prefetch
Professional.xml
Provisioning
regedit.exe
Registration
RemotePackages
rescache
Resources
SchCache
schemas
security
ServiceProfiles
ServiceState
servicing
Setup
setupact.log
setuperr.log
ShellComponents
ShellExperiences
SKB
SoftwareDistribution
Speech
Speech_OneCore
splwow64.exe
System
system.ini
System32
SystemApps
```

```
SystemResources
SystemTemp
SysWOW64
TAPI
Tasks
Temp
tracing

- C$  - (readable,writable)
  + Content of this share :
Documents and Settings
inetpub
Packages
PerfLogs
Program Files
Program Files (x86)
ProgramData
Recovery
swapfile.sys
System Volume Information
temp
Users
Windows
WindowsAzure

- D$  - (readable,writable)
  + Content of this share :
CollectGuestLogsTemp
DATALOSS_WARNING_README.txt
DumpStack.log.tmp
pagefile.sys
System Volume Information
```

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:

Publication date: 2001/10/17, Modification date: 2021/09/20

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```
Nessus was able to obtain the following information about the host, by
parsing the SMB2 Protocol's NTLM SSP message:

 Target Name: notengo
 NetBIOS Domain Name: notengo
 NetBIOS Computer Name: notengo
 DNS Domain Name: notengo
 DNS Computer Name: notengo
 DNS Tree Name: unknown
 Product Version: 10.0.26100
```

21643 - SSL Cipher Suites Supported

Synopsis

The remote service encrypts communications using SSL.

Description

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

See Also

https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

http://www.nessus.org/u?e17ffced

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2006/06/05, Modification date: 2024/09/11

Ports

10.1.0.141 (TCP/3389) Vulnerability State: Resurfaced

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

SSL Version : TLSv13
  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption
 MAC
    ----------------------        ----------       ---           ----     ---------------------
 ---
    TLS_AES_256_GCM_SHA384        0x13, 0x02       -             -        AES-GCM(256)
 SHA384


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

    Name                          Code             KEX           Auth     Encryption
 MAC
    ----------------------        ----------       ---           ----     ---------------------
 ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDHE         RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDHE         RSA      AES-GCM(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
 SHA256
    RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDHE         RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDHE         RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDHE         RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDHE         RSA      AES-CBC(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
 SHA256


SSL Version : TLSv11
  High Strength Ciphers (>= 112-bit key)

 [...]
```

48763 - Microsoft Windows 'CWDIllegalInDllSearch' Registry Setting

Synopsis

CWDIllegalInDllSearch Settings: Improper settings could allow code execution attacks.

Description

Windows Hosts can be hardened against DLL hijacking attacks by setting the The 'CWDIllegalInDllSearch' registry entry in to one of the following settings:
- 0xFFFFFFFF (Removes the current working directory from the default DLL search order)
- 1 (Blocks a DLL Load from the current working directory if the current working directory is set to a WebDAV folder)
- 2 (Blocks a DLL Load from the current working directory if the current working directory is set to a remote folder)

See Also

http://www.nessus.org/u?0c574c56

http://www.nessus.org/u?5234ef0c

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2010/08/26, Modification date: 2019/12/20

Ports

10.1.0.141 (TCP/445) Vulnerability State: Resurfaced

```
  Name  : SYSTEM\CurrentControlSet\Control\Session Manager\CWDIllegalInDllSearch
  Value : Registry Key Empty or Missing
```

48942 - Microsoft Windows SMB Registry : OS Version and Processor Architecture

Synopsis

It was possible to determine the processor architecture, build lab strings, and Windows OS version installed on the remote system.

Description

Nessus was able to determine the processor architecture, build lab strings, and the Windows OS version installed on the remote system by connecting to the remote registry with the supplied credentials.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2010/08/31, Modification date: 2022/02/01

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```
Operating system version = 10.26200
Architecture = x64
Build lab extended = 26100.1.amd64fre.ge_release.240331-1435
```

56984 - SSL / TLS Versions Supported

Synopsis

The remote service encrypts communications.

Description

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

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2011/12/01, Modification date: 2025/06/16

Ports

10.1.0.141 (TCP/3389) Vulnerability State: Active

```
This port supports TLSv1.3/TLSv1.0/TLSv1.1/TLSv1.2.
```

135860 - WMI Not Available

Synopsis

WMI queries could not be made against the remote host.

Description

WMI (Windows Management Instrumentation) is not available on the remote host over DCOM. WMI queries are used to gather information about the remote host, such as its current state, network interface configuration, etc.
Without this information Nessus may not be able to identify installed software or security vunerabilities that exist on the remote host.

See Also

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2020/04/21, Modification date: 2026/01/20

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```
Can't connect to the 'root\CIMV2' WMI namespace.
```

148541 - Windows Language Settings Detection

Synopsis

This plugin enumerates language files on a windows host.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates language IDs listed on the host.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2021/04/14, Modification date: 2022/02/01

Ports

10.1.0.141 (TCP/0) Vulnerability State: Active

```
Default Install Language Code: 1033

Default Active Language Code: 1033

Other common microsoft Language packs may be scanned as well.
```

277654 - TLS Supported Groups

Synopsis

The remote service negotiates TLS supported curve groups.

Description

This plugin detects which TLS supported groups entries are supported by the remote service.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2025/12/08, Modification date: 2026/01/20

Ports

10.1.0.141 (TCP/3389) Vulnerability State: Resurfaced

```

These are the TLS supported groups offered by the remote server :


TLS supported groups :

Name                Code
--------------------------
secp256r1           0x0017
secp384r1           0x0018
x25519              0x001d
```

10335 - Nessus TCP scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a classical TCP port scanner. It shall be reasonably quick even against a firewalled target.
Once a TCP connection is open, it grabs any available banner for the service identification plugins.
Note that TCP scanners are more intrusive than SYN (half open) scanners.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information:

Publication date: 2009/02/04, Modification date: 2025/07/14

Ports

10.1.0.141 (TCP/0) Vulnerability State: Active

```
 {"listening":
[{"port":445,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":"cifs","plugin_output":n
{"port":3389,"protocol":"TCP","interfaces":null,"all_interfaces":false,"service_name":"msrdp","plugin_output":
{"TCP":{"discrete":
[7,9,11,13,15,27,29,31,33,35,333,702,721,723,744,767,808,810,860,871,873,898,927,950,953,975,1005,1008,1010,10
 [...]
```

11457 - Microsoft Windows SMB Registry : Winlogon Cached Password Weakness

Synopsis

User credentials are stored in memory.

Description

The registry key 'HKLM\Software\Microsoft\WindowsNT\CurrentVersion\ Winlogon\CachedLogonsCount' is not 0.
Using a value greater than 0 for the CachedLogonsCount key indicates that the remote Windows host locally caches the passwords of the users when they login, in order to continue to allow the users to login in the case of the failure of the primary domain controller (PDC).
Cached logon credentials could be accessed by an attacker and subjected to brute force attacks.

See Also

http://www.nessus.org/u?184d3eab

http://www.nessus.org/u?fe16cea8

https://technet.microsoft.com/en-us/library/cc957390.aspx

Solution

Consult Microsoft documentation and best practices.

Risk Factor

None

Plugin Information:

Publication date: 2003/03/24, Modification date: 2018/06/05

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```
  Max cached logons : 10
```

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS Base Score

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

Plugin Information:

Publication date: 2012/01/17, Modification date: 2022/06/14

Ports

10.1.0.141 (TCP/3389) Vulnerability State: Active

```
The following certificate was found at the top of the certificate
chain sent by the remote host, but is self-signed and was not
found in the list of known certificate authorities :

|-Subject : CN=notengo
```

58181 - Windows DNS Server Enumeration

Synopsis

Nessus enumerated the DNS servers being used by the remote Windows host.

Description

Nessus was able to enumerate the DNS servers configured on the remote Windows host by looking in the registry.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2012/03/01, Modification date: 2022/02/01

Ports

10.1.0.141 (TCP/445) Vulnerability State: Resurfaced

```
Nessus enumerated DNS servers for the following interfaces :

Interface: {aac2247b-7762-4bdc-938f-d4254cd8bd64}
Network Connection : Ethernet
DhcpNameServer: 168.63.129.16

Interface: Default
DhcpNameServer: 168.63.129.16
```

92365 - Microsoft Windows Hosts File

Synopsis

Nessus was able to collect the hosts file from the remote host.

Description

Nessus was able to collect the hosts file from the remote Windows host and report it as attachment.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2020/01/27

Ports

10.1.0.141 (TCP/0) Vulnerability State: Resurfaced

```
Windows hosts file attached.

MD5: 3688374325b992def12793500307566d
SHA-1: 4bed0823746a2a8577ab08ac8711b79770e48274
SHA-256: 2d6bdfb341be3a6234b24742377f93aa7c7cfb0d9fd64efa9282c87852e57085
```

92368 - Microsoft Windows Scripting Host Settings

Synopsis

Nessus was able to collect and report the Windows scripting host settings from the remote host.

Description

Nessus was able to collect system and user level Windows scripting host settings from the remote Windows host and generate a report as a CSV attachment.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/05/23

Ports

10.1.0.141 (TCP/0) Vulnerability State: Resurfaced

```
HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings\displaylogo : 1
HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings\usewinsafer : 1
HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings\silentterminate : 0
HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings\activedebugging : 1
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\displaylogo : 1
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\usewinsafer : 1
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\silentterminate : 0
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows Script Host\Settings\activedebugging : 1

Windows scripting host configuration attached.
```

92434 - User Download Folder Files

Synopsis

Nessus was able to enumerate downloaded files on the remote host.

Description

Nessus was able to generate a report of all files listed in the default user download folder.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/05/16

Ports

10.1.0.141 (TCP/0) Vulnerability State: Resurfaced

```
C:\\Users\Notengo\Downloads\desktop.ini
C:\\Users\Public\Downloads\desktop.ini

Download folder content report attached.
```

121010 - TLS Version 1.1 Protocol Detection

Synopsis

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

Description

The remote service accepts connections encrypted using TLS 1.1.
TLS 1.1 lacks support for current and recommended cipher suites.
Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1
As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

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

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

Solution

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

Risk Factor

None

References

XREF	CWE-327

Plugin Information:

Publication date: 2019/01/08, Modification date: 2023/04/19

Ports

10.1.0.141 (TCP/3389) Vulnerability State: Resurfaced

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

136318 - TLS Version 1.2 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.2.

See Also

https://tools.ietf.org/html/rfc5246

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2020/05/04, Modification date: 2020/05/04

Ports

10.1.0.141 (TCP/3389) Vulnerability State: Resurfaced

```
TLSv1.2 is enabled and the server supports at least one cipher.
```

187318 - Microsoft Windows Installed

Synopsis

The remote host is running Microsoft Windows.

Description

The remote host is running Microsoft Windows.

See Also

https://www.microsoft.com/en-us/windows

https://www.microsoft.com/en-us/windows-server

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2023/12/27, Modification date: 2026/01/05

Ports

10.1.0.141 (TCP/0) Vulnerability State: Active

```

  OS Name      : Microsoft Windows 11 25H2
  Vendor       : Microsoft
  Product      : Windows
  Release      : 11 25H2
  Edition      : Pro
  Version      : 10.0.26200.7623
  Role         : client
  Kernel       : Windows NT 10.0
  Architecture : x64
  CPE v2.2     : cpe:/o:microsoft:windows_11_25h2:10.0.26200.7623:-:~~pro~~x64~
  CPE v2.3     : cpe:2.3:o:microsoft:windows_11_25h2:10.0.26200.7623:-:*:*:pro:*:x64:*
  Type         : local
  Method       : SMB
  Confidence   : 100
```

277650 - Remote Services Not Using Post-Quantum Ciphers

Synopsis

Reports remote services that do not offer post-quantum ciphers.

Description

This plugin reports network services that do not offer post-quantum ciphers. Tenable makes no attempt to determine whether the remote service would be vulnerable to a post-quantum attack.
However, cryptography that depends on the classic difficulty of solving the discrete logarithm problem or on the classic difficulty of large prime factorization is broken by Shor's algorithm. Examples of this are RSA asymmetric encryption and Diffie-Hellman key exchange.

See Also

http://www.nessus.org/u?7a390f87

http://www.nessus.org/u?ad7d6b3b

http://www.nessus.org/u?1c0c61e0

http://www.nessus.org/u?5eec4b28

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2025/12/08, Modification date: 2025/12/08

Ports

10.1.0.141 (TCP/3389) Vulnerability State: Resurfaced

```
The target TLS server offers no post-quantum ciphers.
```

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:

Publication date: 1999/11/27, Modification date: 2023/12/04

Ports

10.1.0.141 (UDP/0) Vulnerability State: Active

```
For your information, here is the traceroute from 10.0.0.8 to 10.1.0.141 :
10.0.0.8
10.1.0.141

Hop Count: 1
```

10400 - Microsoft Windows SMB Registry Remotely Accessible

Synopsis

Access the remote Windows Registry.

Description

It was possible to access the remote Windows Registry using the login / password combination used for the Windows local checks (SMB tests).

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2025/12/16

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

20811 - Microsoft Windows Installed Software Enumeration (credentialed check)

Synopsis

It is possible to enumerate installed software.

Description

This plugin lists software potentially installed on the remote host by crawling the registry entries in :
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall HKLM\SOFTWARE\Microsoft\Updates

Note that these entries do not necessarily mean the applications are actually installed on the remote host - they may have been left behind by uninstallers, or the associated files may have been manually removed.

Solution

Remove any applications that are not compliant with your organization's acceptable use and security policies.

Risk Factor

None

References

XREF	IAVT-0001-T-0501

Plugin Information:

Publication date: 2006/01/26, Modification date: 2022/02/01

Ports

10.1.0.141 (TCP/445) Vulnerability State: Resurfaced

```
The following software are installed on the remote host :

Microsoft Edge  [version 144.0.3719.104]  [installed on 2026/02/01]
Microsoft Edge Update  [version 1.3.217.3]
Microsoft Edge WebView2 Runtime  [version 144.0.3719.93]  [installed on 2026/01/26]
```

38689 - Microsoft Windows SMB Last Logged On User Disclosure

Synopsis

Nessus was able to identify the last logged on user on the remote host.

Description

By connecting to the remote host with the supplied credentials, Nessus was able to identify the username associated with the last successful logon.
Microsoft documentation notes that interactive console logons change the DefaultUserName registry entry to be the last logged-on user.

See Also

http://www.nessus.org/u?a29751b5

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2009/05/05, Modification date: 2019/09/02

Ports

10.1.0.141 (TCP/445) Vulnerability State: Resurfaced

```
Last Successful logon : .\Administrator
```

62042 - SMB QuickFixEngineering (QFE) Enumeration

Synopsis

The remote host has quick-fix engineering updates installed.

Description

By connecting to the host with the supplied credentials, this plugin enumerates quick-fix engineering updates installed on the remote host via the registry.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2012/09/11, Modification date: 2022/02/01

Ports

10.1.0.141 (TCP/0) Vulnerability State: Resurfaced

```
Here is a list of quick-fix engineering updates installed on the
remote system :

KB5054156, Installed on: 2026/01/09
KB5066128
```

63080 - Microsoft Windows Mounted Devices

Synopsis

It is possible to get a list of mounted devices that may have been connected to the remote system in the past.

Description

By connecting to the remote host with the supplied credentials, this plugin enumerates mounted devices that have been connected to the remote host in the past.

See Also

http://www.nessus.org/u?99fcc329

Solution

Make sure that the mounted drives agree with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2012/11/28, Modification date: 2022/02/01

Ports

10.1.0.141 (TCP/445) Vulnerability State: Resurfaced

```
  Name     : \dosdevices\e:
  Data     : \??\SCSI#CdRom&Ven_Msft&Prod_Virtual_DVD-ROM#5&394b69d0&0&000002#{53f5630d-
b6bf-11d0-94f2-00a0c91efb8b}
  Raw data :
 5c003f003f005c005300430053004900230043006400520006f006d002600560065006e005f004d007300660074002600500072006f006

  Name     : \dosdevices\d:
  Data     : Y
  Raw data : 8a5983bc0000100000000000

  Name     : \??\volume{9c4c207a-f755-11f0-a4af-806e6f6e6963}
  Data     : \??\SCSI#CdRom&Ven_Msft&Prod_Virtual_DVD-ROM#5&394b69d0&0&000002#{53f5630d-
b6bf-11d0-94f2-00a0c91efb8b}
  Raw data :
 5c003f003f005c005300430053004900230043006400520006f006d002600560065006e005f004d007300660074002600500072006f006

  Name     : \dosdevices\c:
  Data     : DMIO:ID:n,Mh$p
  Raw data : 444d494f3a49443a06d46e192cfaca4d891afa1f682470d1
```

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:

Publication date: 2013/02/22, Modification date: 2023/07/10

Ports

10.1.0.141 (TCP/3389) Vulnerability State: Active

```
 Subject Name:

Common Name: notengo

Issuer Name:

Common Name: notengo

Serial Number: 4B 17 CD 0A 47 90 6C 9A 4B 23 FD FA 3D 2C 43 00

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 21 05:47:21 2026 GMT
Not Valid After: Jul 23 05:47:21 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E6 CB BF 25 42 0F BB 92 EA B7 42 56 C9 F2 44 55 52 4C 96
            B5 B7 B5 5B 3B F3 3C B3 24 89 0F AE 1E C9 7E DF 59 A0 56 26
            82 C8 86 F3 73 00 D4 EF 32 17 90 0D 96 A2 FE 6C B3 29 67 E5
            59 EB 5B 94 F8 FD C8 BA 07 E3 4A 8A 09 A4 AD 62 F0 8C 17 C2
            9C CD 6D D9 A8 DC 26 59 67 81 0E 05 9C 31 0B 6F 32 B2 65 07
            55 03 F4 9B 59 F7 62 D3 C9 45 45 84 35 0B 7E AB 6D 44 59 1A
            ED 84 0C AA 45 5E 5D 71 78 D1 EB 6B 29 C9 A3 38 31 9D F2 E1
            9E D0 F8 0C 8C 84 87 10 EF AC A2 FE A3 1F B0 53 75 26 CB 98
            56 0E 47 D5 5A 01 7C 23 27 96 5F 12 DE 76 89 FB A7 CD 88 6D
            41 F4 36 95 03 53 23 53 43 AA 74 8A CC 9C 48 BE 2F AB AD B9
            D7 E6 2B B7 CB 23 A1 E9 48 BE 9C 3A 8B C9 C2 48 AB 9A 78 2B
            B0 E1 C3 1A 4A 1A E1 28 36 61 90 14 8F 90 60 CA EE 3A 09 2B
            36 54 C7 07 CF 81 CD 17 AB C6 E8 2E 0D 10 10 3B 21
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 42 C7 85 33 4E 0C CD 08 D6 07 80 7B 73 BE A5 68 BE 8F 95
           36 37 F8 F7 E5 B2 75 A0 E7 31 73 D7 C8 EA 6E F0 D0 60 F6 8B
           E9 68 4D A4 1C 5E 57 94 CA E4 F8 80 0F 7A E4 23 5A 31 26 CD
           A2 D3 3A 7F 31 CC B4 13 F9 65 88 D6 EA EB 9D 01 FA 16 7E 64
           B2 43 2F BE 3E AA 78 3E A4 B3 BB 43 89 CE 66 95 AC BC BF 4D
           75 3D 9B DD 19 38 C0 A9 A9 BE 37 85 E5 FB E7 93 B7 C2 04 75
           53 28 95 13 F9 BA CB 14 2F F6 0B 4C 53 00 AF 53 D1 B7 58 CC
           D2 2F 15 4F 3E 37 68 07 FF 93 9E 98 39 D0 E4 F5 44 AB FA 2F
           30 1F A8 50 B4 3E D2 9D 83 8D D5 09 86 6E 3E D9 87 C6 1F B0
           F6 66 8B 87 63 50 66 9A B5 A7 E2 [...]
```

92364 - Microsoft Windows Environment Variables

Synopsis

Nessus was able to collect and report environment variables from the remote host.

Description

Nessus was able to collect system and active account environment variables on the remote Windows host and generate a report as a CSV attachment.

Solution

N/A

Risk Factor

None

References

XREF	IAVT-0001-T-0757

Plugin Information:

Publication date: 2016/07/19, Modification date: 2026/01/29

Ports

10.1.0.141 (TCP/0) Vulnerability State: Resurfaced

```
Global Environment Variables :
  processor_level : 6
  comspec : %SystemRoot%\system32\cmd.exe
  number_of_processors : 1
  username : SYSTEM
  os : Windows_NT
  temp : %SystemRoot%\TEMP
  processor_revision : 5507
  path : %SystemRoot%\system32;%SystemRoot%;%SystemRoot%\System32\Wbem;%SYSTEMROOT%
\System32\WindowsPowerShell\v1.0\;%SYSTEMROOT%\System32\OpenSSH\
  tmp : %SystemRoot%\TEMP
  processor_identifier : Intel64 Family 6 Model 85 Stepping 7, GenuineIntel
  driverdata : C:\Windows\System32\Drivers\DriverData
  pathext : .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
  processor_architecture : AMD64
  psmodulepath : %ProgramFiles%\WindowsPowerShell\Modules;%SystemRoot%\system32\WindowsPowerShell
\v1.0\Modules
  windir : %SystemRoot%

Active User Environment Variables
  - S-1-5-21-1658136452-1347933459-2279167012-500
    userdomain : notengo
    username : Notengo
    temp : %USERPROFILE%\AppData\Local\Temp
    path : %USERPROFILE%\AppData\Local\Microsoft\WindowsApps;
    logonserver : \\notengo
    localappdata : C:\Users\Notengo\AppData\Local
    tmp : %USERPROFILE%\AppData\Local\Temp
    homedrive : C:
    homepath : \Users\Notengo
    userdomain_roamingprofile : notengo
    userprofile : C:\Users\Notengo
    onedrive : C:\Users\Notengo\OneDrive
    appdata : C:\Users\Notengo\AppData\Roaming
```

92421 - Internet Explorer Typed URLs

Synopsis

Nessus was able to enumerate URLs that were manually typed into the Internet Explorer address bar.

Description

Nessus was able to generate a list URLs that were manually typed into the Internet Explorer address bar.

See Also

https://forensafe.com/blogs/typedurls.html

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2024/05/08

Ports

10.1.0.141 (TCP/0) Vulnerability State: Resurfaced

```
http://go.microsoft.com/fwlink/p/?LinkId=255141

Internet Explorer typed URL report attached.
```

92435 - UserAssist Execution History

Synopsis

Nessus was able to enumerate program execution history on the remote host.

Description

Nessus was able to gather evidence from the UserAssist registry key that has a list of programs that have been executed.

See Also

https://www.nirsoft.net/utils/userassist_view.html

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2019/11/12

Ports

10.1.0.141 (TCP/0) Vulnerability State: Resurfaced

```
microsoft.autogenerated.{8abd94fb-e7d6-84a6-a997-c918edde0ae5}
microsoft.screensketch_8wekyb3d8bbwe!app
{0139d44e-6afe-49f2-8690-3dafcae6ffb8}\administrative tools\computer management.lnk
{a77f5d77-2e2b-44c3-a6a2-aba601054a51}\windows powershell\windows powershell.lnk
microsoft.windowscalculator_8wekyb3d8bbwe!app
microsoft.windowsterminal_8wekyb3d8bbwe!app
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\mmc.exe
microsoft.windowsfeedbackhub_8wekyb3d8bbwe!app
microsoftwindows.client.cbs_cw5n1h2txyewy!webexperiencehost
{9e3995ab-1f9c-4f13-b827-48b24b6c7174}\taskbar\file explorer.lnk
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\windowspowershell\v1.0\powershell.exe
microsoft.paint_8wekyb3d8bbwe!app
microsoft.autogenerated.{bd3f924e-55fb-a1ba-9de6-b50f9f2460ac}
microsoft.windows.shell.rundialog
microsoft.windowsnotepad_8wekyb3d8bbwe!app
microsoft.windows.startmenuexperiencehost_cw5n1h2txyewy!fulltrustapp
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\wf.msc
microsoft.microsoftstickynotes_8wekyb3d8bbwe!app
microsoft.xboxgamingoverlay_8wekyb3d8bbwe!app
ueme_ctlcuacount:ctor
msedge
microsoft.windows.cloudexperiencehost_cw5n1h2txyewy!app
microsoft.windowsstore_8wekyb3d8bbwe!app
microsoft.windows.explorer
ueme_ctlsession
microsoft.windows.shellexperiencehost_cw5n1h2txyewy!app
{1ac14e77-02e7-4e5d-b744-2eb1ae5198b7}\msinfo32.exe
microsoftwindows.client.cbs_cw5n1h2txyewy!cortanaui

Extended userassist report attached.
```

131023 - Windows Defender Installed

Synopsis

Windows Defender is installed on the remote Windows host.

Description

Windows Defender, an antivirus component of Microsoft Windows is installed on the remote Windows host.

See Also

https://www.microsoft.com/en-us/windows/comprehensive-security

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2019/11/15, Modification date: 2026/01/20

Ports

10.1.0.141 (TCP/0) Vulnerability State: Resurfaced

```
  Path                            : C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.25110.6-0\
  Version                         : 4.18.25110.6
  Engine Version              : 1.1.25110.1
  Malware Signature Timestamp : Feb.  4, 2026 at 18:23:34 GMT
  Malware Signature Version   : 1.443.1006.0
  Signatures Last Updated     : Feb.  5, 2026 at 01:30:17 GMT
```

138330 - TLS Version 1.3 Protocol Detection

Synopsis

The remote service encrypts traffic using a version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.3.

See Also

https://tools.ietf.org/html/rfc8446

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2020/07/09, Modification date: 2023/12/13

Ports

10.1.0.141 (TCP/3389) Vulnerability State: Resurfaced

```
TLSv1.3 is enabled and the server supports at least one cipher.
```

280146 - Microsoft Azure Guest Agent Installed (Windows)

Synopsis

Microsoft Azure Guest Agent is installed on the remote Windows host.

Description

Microsoft Azure Guest Agent is installed on the remote Windows host.

See Also

http://www.nessus.org/u?4da9ec88

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2025/12/30, Modification date: 2026/01/20

Ports

10.1.0.141 (TCP/0) Vulnerability State: Active

```
  Path    : C:\WindowsAzure\GuestAgent_2.7.41491.1183_2026-01-22_055123\CollectVMHealth.exe
  Version : 2.7.41491.1183
```

10395 - Microsoft Windows SMB Shares Enumeration

Synopsis

It is possible to enumerate remote network shares.

Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2022/02/01

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```
Here are the SMB shares available on the remote host when logged in as Notengo:

  - ADMIN$
  - C$
  - D$
  - IPC$
```

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :
- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS Base Score

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

Plugin Information:

Publication date: 2010/12/15, Modification date: 2025/06/16

Ports

10.1.0.141 (TCP/3389) Vulnerability State: Active

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : CN=notengo
|-Issuer  : CN=notengo
```

70544 - SSL Cipher Block Chaining Cipher Suites Supported

Synopsis

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

Description

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

See Also

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

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

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

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2013/10/22, Modification date: 2021/02/03

Ports

10.1.0.141 (TCP/3389) Vulnerability State: Resurfaced

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption
 MAC
    ----------------------        ----------       ---           ----     ---------------------
 ---
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDHE         RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDHE         RSA      AES-CBC(256)
 SHA1
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDHE         RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDHE         RSA      AES-CBC(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
 SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

92424 - MUICache Program Execution History

Synopsis

Nessus was able to enumerate recently executed programs on the remote host.

Description

Nessus was able to query the MUIcache registry key to find evidence of program execution.

See Also

https://forensicartifacts.com/2010/08/registry-muicache/

http://windowsir.blogspot.com/2005/12/mystery-of-muicachesolved.html

http://www.nirsoft.net/utils/muicache_view.html

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/05/16

Ports

10.1.0.141 (TCP/0) Vulnerability State: Active

```
 c:\windows\system32\fsquirt.exe.applicationcompany : Microsoft Corporation
c:\windows\system32\rgnupdt.exe.friendlyappname : rgnupdt
c:\windows\system32\shell32.dll.applicationcompany : Microsoft Corporation
c:\windows\explorer.exe.friendlyappname : Windows Explorer
c:\windows\explorer.exe.applicationcompany : Microsoft Corporation
langid :  .
c:\windows\system32\mmc.exe.friendlyappname : Microsoft Management Console
c:\windows\system32\appresolver.dll.applicationcompany : Microsoft Corporation
c:\windows\system32\shell32.dll.friendlyappname : Windows Shell Common Dll
c:\windows\system32\fsquirt.exe.friendlyappname : fsquirt
c:\windows\system32\rgnupdt.exe.applicationcompany : Microsoft Corporation
c:\windows\system32\mmc.exe.applicationcompany : Microsoft Corporation
c:\windows\system32\appresolver.dll.friendlyappname : App Resolver
@%systemroot%\system32\fveui.dll,-843 : BitLocker Drive Encryption
@%systemroot%\system32\fveui.dll,-844 : BitLocker Data Recovery Agent
@%systemroot%\system32\sppcomapi.dll,-3200 : Software Licensing
@%systemroot%\system32\ci.dll,-100 : Isolated User Mode (IUM)
@%systemroot%\system32\ngcrecovery.dll,-100 : Windows Hello Recovery Key Encryption
@c:\programdata\microsoft\windows defender\platform\4.18.25110.6-0\mpasdesc.dll,-330 : Microsoft
 Defender Antivirus Mini-Filter Driver
@%systemroot%\system32\dnsapi.dll,-103 : Domain Name System (DNS) Server Trust
@%systemroot%\system32\ci.dll,-101 : Enclave
@%systemroot%\system32\firewallcontrolpanel.dll,-12122 : Windows Defender Firewall
@%systemroot%\system32\wuaueng.dll,-400 : Windows Update
@%systemroot%\system32\windowspowershell\v1.0\powershell.exe,-124 : Document Encryption
@%systemroot%\system32\fveui.dll,-843 : BitLocker Drive Encryption
@%systemroot%\system32\fveui.dll,-844 : BitLocker Data Recovery Agent
c:\windows\system32,@elscore.dll,-9 : Microsoft Bengali to Latin Transliteration
c:\windows\system32,@elscore.dll,-5 : Microsoft Transliteration Engine
@%systemroot%\system32\ci.dll,-100 : Isolated User Mode (IUM)
c:\windows\system32,@elscore.dll,-4 [...]
```

92426 - OpenSaveMRU History

Synopsis

Nessus was able to enumerate opened and saved files on the remote host.

Description

Nessus was able to generate a report on files that were opened using the shell dialog box or saved using the shell dialog box. This is the box that appears when you attempt to save a document or open a document in Windows Explorer.

See Also

http://www.nessus.org/u?ac4dd3fb

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/05/23

Ports

10.1.0.141 (TCP/0) Vulnerability State: Active

```
Open / Save report attached.
```

117885 - Target Credential Issues by Authentication Protocol - Intermittent Authentication Failure

Synopsis

Nessus was able to log in to the remote host using the provided credentials, but there were intermittent authentication failures.

Description

Nessus was able to successfully authenticate to the remote host on an authentication protocol at least once using credentials provided in the scan policy.
However, one or more plugins failed to authenticate to the remote host on the same port and protocol using the same credential set that was previously successful. This may indicate an intermittent authentication problem with the remote host, which could be caused by session rate limits, session concurrency limits, or other issues preventing consistent authentication success.
These intermittent authentication failures may have affected the results of some plugins. See plugin output for failure details.

Solution

N/A

Risk Factor

None

References

XREF	IAVB-0001-B-0509

Plugin Information:

Publication date: 2018/10/02, Modification date: 2024/03/25

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```

Nessus was able to successfully log into the remote host as :

User:       '10.1.0.141\Notengo'
Port:       445
Proto:      SMB
Method:     password


Successful authentication was reported by the following plugin :

  Plugin      : smb_login.nasl
  Plugin ID   : 10394
  Plugin Name : Microsoft Windows SMB Log In Possible

However, one or more subsequent plugins failed to authenticate to the
remote host on the same port and protocol using the same credential
set that previously succeeded. This may indicate an intermittent
authentication problem with the remote host which may have affected
the results of the following plugins.

Error message statistics :

  3 Failed to open a socket on port 445. This failure may have prevented
    a login attempt. The failure references the previously successful
    login account for tracking purposes.


Failure Details :

  - Plugin      : microsoft_windows_office_recent.nasl
    Plugin ID   : 92425
    Plugin Name : Microsoft Office File History
    Message     :
Failed to open a socket on port 445. This failure may have prevented
a login attempt. The failure references the previously successful
login account for tracking purposes.
```

```
  - Plugin      : microsoft_windows_mru_exe_registry.nasl
    Plugin ID   : 92423
    Plugin Name : Windows Explorer Recently Executed Programs
    Message     :
Failed to open a socket on port 445. This failure may have prevented
a login attempt. The failure references the previously successful
login account for tracking purposes.


  - Plugin      : microsoft_windows_mapped_network_drives_mru.nasl
    Plugin ID   : 92422
    Plugin Name : Windows Mapped Network Drives
    Message     :
Failed to open a socket on port 445. This failure may have prevented
a login attempt. The failure references the previously successful
login account for tracking purposes.
```

141118 - Target Credential Status by Authentication Protocol - Valid Credentials Provided

Synopsis

Valid credentials were provided for an available authentication protocol.

Description

Nessus was able to determine that valid credentials were provided for an authentication protocol available on the remote target because it was able to successfully authenticate directly to the remote target using that authentication protocol at least once. Authentication was successful because the authentication protocol service was available remotely, the service was able to be identified, the authentication protocol was able to be negotiated successfully, and a set of credentials provided in the scan policy for that authentication protocol was accepted by the remote service. See plugin output for details, including protocol, port, and account.
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

Plugin Information:

Publication date: 2020/10/15, Modification date: 2024/03/25

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```

Nessus was able to log in to the remote host via the following :

User:       '10.1.0.141\Notengo'
Port:       445
Proto:      SMB
Method:     password
```

157288 - TLS Version 1.1 Deprecated Protocol

Synopsis

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

Description

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1
As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

See Also

https://datatracker.ietf.org/doc/html/rfc8996

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

Solution

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

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

6.1 (AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF	CWE-327

Plugin Information:

Publication date: 2022/04/04, Modification date: 2024/05/14

Ports

10.1.0.141 (TCP/3389) Vulnerability State: Resurfaced

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

162560 - Microsoft Internet Explorer Installed

Synopsis

A web browser is installed on the remote Windows host.

Description

Microsoft Internet Explorer, a web browser bundled with Microsoft Windows, is installed on the remote Windows host.

See Also

https://support.microsoft.com/products/internet-explorer

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2022/06/28, Modification date: 2026/01/07

Ports

10.1.0.141 (TCP/0) Vulnerability State: Active

```

  Path    : C:\Windows\system32\mshtml.dll
  Version : 11.0.26100.7309
```

178102 - Microsoft Windows Installed Software Version Enumeration

Synopsis

Enumerates installed software versions.

Description

This plugin enumerates the installed software version by interrogating information obtained from various registry entries and files on disk. This plugin provides a best guess at the software version and a confidence level for that version.
Note that the versions detected here do not necessarily indicate the actual installed version nor do they necessarily mean that the application is actually installed on the remote host. In some cases there may be artifacts left behind by uninstallers on the system.

Solution

Remove any applications that are not compliant with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2023/07/10, Modification date: 2024/07/15

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```

The following software information is available on the remote host :

 - Microsoft Edge WebView2 Runtime
     Best Confidence Version  : 144.0.3719.93
     Version Confidence Level : 3
     All Possible Versions    :  144.0.3719.93
     Other Version Data
       [InstallDate] :
           Raw Value           : 2026/01/26
       [DisplayIcon] :
           Raw Value           : C:\Program Files (x86)\Microsoft\EdgeWebView\Application
\144.0.3719.93\msedgewebview2.exe,0
           Parsed File Path    : C:\Program Files (x86)\Microsoft\EdgeWebView\Application
\144.0.3719.93\msedgewebview2.exe
           Parsed File Version : 144.0.3719.93
       [InstallLocation] :
           Raw Value           : C:\Program Files (x86)\Microsoft\EdgeWebView\Application
       [UninstallString] :
           Raw Value           : "C:\Program Files (x86)\Microsoft\EdgeWebView\Application
\144.0.3719.93\Installer\setup.exe" --uninstall --msedgewebview --system-level --verbose-logging
           Parsed File Path    : C:\Program Files (x86)\Microsoft\EdgeWebView\Application
\144.0.3719.93\Installer\setup.exe
           Parsed File Version : 144.0.3719.93
       [VersionMinor] :
           Raw Value           : 93
       [Version] :
           Raw Value           : 144.0.3719.93
       [VersionMajor] :
           Raw Value           : 3719
       [DisplayVersion] :
           Raw Value           : 144.0.3719.93
       [DisplayName] :
           Raw Value           : Microsoft Edge WebView2 Runtime

 - Microsoft Edge
     Best Confidence Version  : 144.0.3719.104
     Version Confidence Level : 3
     All Possible Versions    :  144.0.3719.104
     Other Version Data
       [InstallDate] :
           Raw Value           : 2026/02/01
       [DisplayIcon] :
           Raw Value           : C:\Program Files (x86)\Microsoft\Edge\Application
\144.0.3719.104\msedge.exe,0
           Parsed File Path    : C:\Program Files (x86)\Microsoft\Edge\Application
\144.0.3719.104\msedge.exe
           Parsed File Version : 144.0.3719.104
       [InstallLocation] [...]
```

200493 - Microsoft Windows Start Menu Software Version Enumeration

Synopsis

Enumerates Start Menu software versions.

Description

This plugin enumerates the installed software version by interrogating information obtained from various registry entries and files on disk. This plugin provides a best guess at the software version and a confidence level for that version.
Note that the versions detected here do not necessarily indicate the actual installed version nor do they necessarily mean that the application is actually installed on the remote host. In some cases there may be artifacts left behind by uninstallers on the system.

Solution

Remove any applications that are not compliant with your organization's acceptable use and security policies.

Risk Factor

None

Plugin Information:

Publication date: 2024/06/13, Modification date: 2026/01/20

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```
The following software information is available on the remote host :
```

10394 - Microsoft Windows SMB Log In Possible

Synopsis

It was possible to log into the remote host.

Description

The remote host is running a Microsoft Windows operating system or Samba, a CIFS/SMB server for Unix. It was possible to log into it using one of the following accounts :
- Guest account
- Supplied credentials

See Also

http://www.nessus.org/u?5c2589f6

https://support.microsoft.com/en-us/help/246261

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2000/05/09, Modification date: 2025/07/21

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```
- The SMB tests will be done as Notengo/******
```

10859 - Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration

Synopsis

It is possible to obtain the host SID for the remote host.

Description

By emulating the call to LsaQueryInformationPolicy(), it was possible to obtain the host SID (Security Identifier). The host SID can then be used to get the list of local users.

See Also

http://technet.microsoft.com/en-us/library/bb418944.aspx

Solution

You can prevent anonymous lookups of the host SID by setting the 'RestrictAnonymous' registry setting to an appropriate value.
Refer to the 'See also' section for guidance.

Risk Factor

None

Plugin Information:

Publication date: 2002/02/13, Modification date: 2024/01/31

Ports

10.1.0.141 (TCP/445) Vulnerability State: Resurfaced

```
The remote host SID value is : S-1-5-21-1658136452-1347933459-2279167012

The value of 'RestrictAnonymous' setting is : 0
```

72367 - Microsoft Internet Explorer Version Detection

Synopsis

Internet Explorer is installed on the remote host.

Description

The remote Windows host contains Internet Explorer, a web browser created by Microsoft.

See Also

https://support.microsoft.com/en-us/help/17621/internet-explorer-downloads

Solution

N/A

Risk Factor

None

References

XREF	IAVT-0001-T-0509

Plugin Information:

Publication date: 2014/02/06, Modification date: 2022/02/01

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```
  Version  : 11.1882.26100.0
```

92431 - User Shell Folders Settings

Synopsis

Nessus was able to find the folder paths for user folders on the remote host.

Description

Nessus was able to gather a list of settings from the target system that store common user folder locations. A few of the more common locations are listed below :

- Administrative Tools
- AppData
- Cache
- CD Burning
- Cookies
- Desktop
- Favorites
- Fonts
- History
- Local AppData
- My Music
- My Pictures
- My Video
- NetHood
- Personal
- PrintHood
- Programs
- Recent
- SendTo
- Start Menu
- Startup
- Templates

See Also

https://technet.microsoft.com/en-us/library/cc962613.aspx

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/05/16

Ports

10.1.0.141 (TCP/0) Vulnerability State: Resurfaced

```
 Notengo
  - {7d1d3a04-debb-4115-95cf-2f29da2920da} : C:\Users\Notengo\Searches
  - {1b3ea5dc-b587-4786-b4ef-bd1dc332aeae} : C:\Users\Notengo\AppData\Roaming\Microsoft\Windows
\Libraries
  - {374de290-123f-4565-9164-39c4925e467b} : C:\Users\Notengo\Downloads
  - recent : C:\Users\Notengo\AppData\Roaming\Microsoft\Windows\Recent
  - my video : C:\Users\Notengo\Videos
  - my music : C:\Users\Notengo\Music
  - {56784854-c6cb-462b-8169-88e350acb882} : C:\Users\Notengo\Contacts
  - {bfb9d5e0-c6a9-404c-b2b2-ae6db6af4968} : C:\Users\Notengo\Links
  - {a520a1a4-1780-4ff6-bd18-167343c5af16} : C:\Users\Notengo\AppData\LocalLow
  - sendto : C:\Users\Notengo\AppData\Roaming\Microsoft\Windows\SendTo
  - start menu : C:\Users\Notengo\AppData\Roaming\Microsoft\Windows\Start Menu
  - cookies : C:\Users\Notengo\AppData\Local\Microsoft\Windows\INetCookies
  - personal : C:\Users\Notengo\Documents
  - administrative tools : C:\Users\Notengo\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
\Administrative Tools
  - startup : C:\Users\Notengo\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
  - nethood : C:\Users\Notengo\AppData\Roaming\Microsoft\Windows\Network Shortcuts
  - history : C:\Users\Notengo\AppData\Local\Microsoft\Windows\History
  - {4c5c32ff-bb9d-43b0-b5b4-2d72e54eaaa4} : C:\Users\Notengo\Saved Games
  - {00bcfc5a-ed94-4e48-96a1-3f6217f21990} : C:\Users\Notengo\AppData\Local\Microsoft\Windows
\RoamingTiles
  - !do not use this registry key : Use the SHGetFolderPath or SHGetKnownFolderPath function
 instead
  - local appdata : C:\Users\Notengo\AppData\Local
  - my pictures : C:\Users\Notengo\Pictures
  - templates : C:\Users\Notengo\AppData\Roaming\Microsoft\Windows\Templates
  - printhood : C:\Users\Notengo\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
  - cache : C:\Users\Notengo\AppData\Local\Microsoft\Windows\INetCache
  - desktop : C:\Users\Notengo\Desktop
  - programs : C:\Users\Notengo\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
  - fonts : C:\Windows\Fonts
  - cd burning : C:\Users\Notengo\AppData\Local\Microsoft\Windows\Burn\Burn
 [...]
```

93962 - Microsoft Security Rollup Enumeration

Synopsis

This plugin enumerates installed Microsoft security rollups.

Description

Nessus was able to enumerate the Microsoft security rollups installed on the remote Windows host.

See Also

http://www.nessus.org/u?b23205aa

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/10/11, Modification date: 2025/11/18

Ports

10.1.0.141 (TCP/445) Vulnerability State: Resurfaced

```

 Cumulative Rollup : 01_2026_2
 Cumulative Rollup : 12_2025
```

```
Cumulative Rollup : 11_2025
Cumulative Rollup : 10_2025

Latest effective update level : 01_2026_2
File checked                  : C:\Windows\system32\bcrypt.dll
File version                  : 10.0.26100.7623
Associated KB                 : 5074109
```

104743 - TLS Version 1.0 Protocol Detection

Synopsis

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

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.
As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.
PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

See Also

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

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

CVSS v3.0 Base Score

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

CVSS Base Score

6.1 (AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF	CWE-327

Plugin Information:

Publication date: 2017/11/22, Modification date: 2023/04/19

Ports

10.1.0.141 (TCP/3389) Vulnerability State: Resurfaced

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

136969 - Microsoft Edge Chromium Installed

Synopsis

Microsoft Edge (Chromium-based) is installed on the remote host.

Description

Microsoft Edge (Chromium-based), a Chromium-based web browser, is installed on the remote host.

See Also

https://www.microsoft.com/en-us/edge

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2020/05/29, Modification date: 2026/01/07

Ports

10.1.0.141 (TCP/445) Vulnerability State: Resurfaced

```
  Path    : C:\Program Files (x86)\Microsoft\Edge\Application
  Version : 144.0.3719.104
  Channel : stable
```

10902 - Microsoft Windows 'Administrators' Group User List

Synopsis

There is at least one user in the 'Administrators' group.

Description

Using the supplied credentials, it is possible to extract the member list of the 'Administrators' group. Members of this group have complete access to the remote system.

Solution

Verify that each member of the group should have this type of access.

Risk Factor

None

Plugin Information:

Publication date: 2002/03/15, Modification date: 2018/05/16

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```

The following users are members of the 'Administrators' group :

  - notengo\Notengo (User)
  - notengo\Administrator (User)
  - notengo\DisabledGuest_01 (User)
```

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:

Publication date: 2002/04/20, Modification date: 2023/08/21

Ports

10.1.0.141 (TCP/3389) Vulnerability State: Active

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:

Publication date: 2005/08/26, Modification date: 2025/10/29

Ports

10.1.0.141 (TCP/0) Vulnerability State: Active

```
Information about this scan :

Nessus version : 10.11.1
Nessus build : 20021
Plugin feed version : 202602041423
Scanner edition used : Nessus
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : MN STIG
Scan policy used : MN STIG
Scanner IP : 10.0.0.8
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 15.625 ms
Thorough tests : yes
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 : yes, as '10.1.0.141\Notengo' via SMB
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2026/2/5 6:30 UTC
Scan duration : 1424 sec
Scan for malware : no
```

25220 - TCP/IP Timestamps Supported

Synopsis

The remote service implements TCP timestamps.

Description

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

See Also

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

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2007/05/16, Modification date: 2023/10/17

Ports

10.1.0.141 (TCP/0) Vulnerability State: Active

42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure

Synopsis

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

Description

The remote host listens on tcp port 445 and replies to SMB requests.
By sending an NTLMSSP authentication request it is possible to obtain the name of the remote system and the name of its domain.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2009/11/06, Modification date: 2019/11/22

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```
The following 2 NetBIOS names have been gathered :

 notengo           = Computer name
 notengo           = Workgroup / Domain name
```

44401 - Microsoft Windows SMB Service Config Enumeration

Synopsis

It was possible to enumerate configuration parameters of remote services.

Description

Nessus was able to obtain, via the SMB protocol, the launch parameters of each active service on the remote host (executable path, logon type, etc.).

Solution

Ensure that each service is configured properly.

Risk Factor

None

References

XREF	IAVT-0001-T-0752

Plugin Information:

Publication date: 2010/02/05, Modification date: 2022/05/16

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```
The following services are set to start automatically :

  AppXSvc startup parameters :
    Display name : AppX Deployment Service (AppXSVC)
    Service name : AppXSvc
    Log on as : LocalSystem
    Executable path : C:\Windows\system32\svchost.exe -k wsappx -p
    Dependencies : rpcss/staterepository/

  AudioEndpointBuilder startup parameters :
    Display name : Windows Audio Endpoint Builder
    Service name : AudioEndpointBuilder
    Log on as : LocalSystem
    Executable path : C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p

  Audiosrv startup parameters :
    Display name : Windows Audio
    Service name : Audiosrv
    Log on as : NT AUTHORITY\LocalService
    Executable path : C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
    Dependencies : AudioEndpointBuilder/RpcSs/

  BFE startup parameters :
    Display name : Base Filtering Engine
    Service name : BFE
    Log on as : NT AUTHORITY\LocalService
    Executable path : C:\Windows\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p
    Dependencies : RpcSs/

  BrokerInfrastructure startup parameters :
    Display name : Background Tasks Infrastructure Service
    Service name : BrokerInfrastructure
    Log on as : LocalSystem
    Executable path : C:\Windows\system32\svchost.exe -k DcomLaunch -p
    Dependencies : RpcEptMapper/DcomLaunch/RpcSs/

  CDPSvc startup parameters :
    Display name : Connected Devices Platform Service
    Service name : CDPSvc
    Log on as : NT AUTHORITY\LocalService
    Executable path : C:\Windows\system32\svchost.exe -k LocalService -p
    Dependencies : ncbservice/RpcSS/Tcpip/

  CDPUserSvc_a6ea3 startup parameters :
    Display name : Connected Devices Platform User Service_a6ea3
    Service name : CDPUserSvc_a6ea3
    Executable path : C:\Windows\system32\svchost.exe -k UnistackSvcGroup

  CoreMessagingRegistrar startup parameters :
    Display name : CoreMessaging
    Service name : CoreMessagingRegistrar
    Log on as : NT AUTHORITY\LocalService
    Executable path : C:\Windows\system32\svchost.exe [...]
```

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:

Publication date: 2010/04/21, Modification date: 2026/01/05

Ports

10.1.0.141 (TCP/0) Vulnerability State: Active

```
The remote operating system matched the following CPE :
  cpe:/o:microsoft:windows_11 -> Microsoft Windows 11

Following application CPE's matched on the remote system :

  cpe:/a:microsoft:.net_framework:4.8.1 -> Microsoft .NET Framework
  cpe:/a:microsoft:edge:144.0.3719.104 -> Microsoft Edge
  cpe:/a:microsoft:ie:11.1882.26100.0 -> Microsoft Internet Explorer
  cpe:/a:microsoft:internet_explorer:11.0.26100.7309 -> Microsoft Internet Explorer
  cpe:/a:microsoft:onedrive:26.2.105.1 -> Microsoft OneDrive
  cpe:/a:microsoft:remote_desktop_connection:10.0.26100.7623 -> Microsoft Remote Desktop
 Connection
  cpe:/a:microsoft:system_center_endpoint_protection:4.18.25110.6 -> Microsoft System Center
 Endpoint Protection
  cpe:/a:microsoft:windows_defender:4.18.25110.6 -> Microsoft Windows Defender
  x-cpe:/a:microsoft:azure_guest_agent:2.7.41491.1183
```

51351 - Microsoft .NET Framework Detection

Synopsis

A software framework is installed on the remote host.

Description

Microsoft .NET Framework, a software framework for Microsoft Windows operating systems, is installed on the remote host.

See Also

https://www.microsoft.com/net

http://www.nessus.org/u?15ae6806

Solution

N/A

Risk Factor

None

References

XREF	IAVT-0001-T-0655

Plugin Information:

Publication date: 2010/12/20, Modification date: 2025/10/15

Ports

10.1.0.141 (TCP/445) Vulnerability State: Resurfaced

```
Nessus detected 2 installs of Microsoft .NET Framework:

  Path         : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\
  Version      : 4.8.1
  Full Version : 4.8.09221
  Install Type : Full
  Release      : 533509

  Path         : C:\Windows\Microsoft.NET\Framework64\v4.0.30319\
  Version      : 4.8.1
  Full Version : 4.8.09221
  Install Type : Client
  Release      : 533509
```

66424 - Microsoft Malicious Software Removal Tool Installed

Synopsis

An antimalware application is installed on the remote Windows host.

Description

The Microsoft Malicious Software Removal Tool is installed on the remote host. This tool is an application that attempts to detect and remove known malware from Windows systems.

See Also

http://www.nessus.org/u?47a3e94d

https://support.microsoft.com/en-us/help/891716

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2013/05/15, Modification date: 2023/01/10

Ports

10.1.0.141 (TCP/445) Vulnerability State: Resurfaced

```
  File                : C:\Windows\system32\MRT.exe
  Version             : 5.138.25120.1002
  Release at last run : unknown
  Report infection information to Microsoft : Yes
```

92415 - Application Compatibility Cache

Synopsis

Nessus was able to gather application compatibility settings on the remote host.

Description

Nessus was able to generate a report on the application compatibility cache on the remote Windows host.

See Also

https://dl.mandiant.com/EE/library/Whitepaper_ShimCacheParser.pdf

http://www.nessus.org/u?4a076105

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/05/23

Ports

10.1.0.141 (TCP/0) Vulnerability State: Active

```
Application compatibility cache report attached.
```

103871 - Microsoft Windows Network Adapters

Synopsis

Identifies the network adapters installed on the remote host.

Description

Using the supplied credentials, this plugin enumerates and reports the installed network adapters on the remote Windows host.

Solution

Make sure that all of the installed network adapters agrees with your organization's acceptable use and security policies.

Risk Factor

None

References

XREF	IAVT-0001-T-0758

Plugin Information:

Publication date: 2017/10/17, Modification date: 2022/02/01

Ports

10.1.0.141 (TCP/445) Vulnerability State: Resurfaced

```
Network Adapter Driver Description : Mellanox ConnectX-4 Lx Virtual Ethernet Adapter
Network Adapter Driver Version     : 23.4.26054.1

Network Adapter Driver Description : Mellanox ConnectX-5 Virtual Adapter
Network Adapter Driver Version     : 23.4.26054.1

Network Adapter Driver Description : Mellanox ConnectX-4 Lx Virtual Ethernet Adapter
Network Adapter Driver Version     : 23.4.26054.1

Network Adapter Driver Description : Mellanox ConnectX-4 Lx Virtual Ethernet Adapter
Network Adapter Driver Version     : 23.4.26054.1

Network Adapter Driver Description : Mellanox ConnectX-4 Lx Virtual Ethernet Adapter
Network Adapter Driver Version     : 23.4.26054.1

Network Adapter Driver Description : Mellanox ConnectX-4 Lx Virtual Ethernet Adapter
Network Adapter Driver Version     : 23.4.26054.1

Network Adapter Driver Description : Mellanox ConnectX-5 Virtual Adapter
Network Adapter Driver Version     : 23.4.26054.1

Network Adapter Driver Description : Mellanox ConnectX-5 Virtual Adapter
Network Adapter Driver Version     : 23.4.26054.1

Network Adapter Driver Description : Mellanox ConnectX-5 Virtual Adapter
Network Adapter Driver Version     : 23.4.26054.1

Network Adapter Driver Description : Mellanox ConnectX-5 Virtual Adapter
Network Adapter Driver Version     : 23.4.26054.1

Network Adapter Driver Description : Mellanox ConnectX-4 Lx Virtual Ethernet Adapter
Network Adapter Driver Version     : 23.4.26054.1
```

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)

Synopsis

It was possible to obtain information about the dialects of SMB2 and SMB3 available on the remote host.

Description

Nessus was able to obtain the set of SMB2 and SMB3 dialects running on the remote host by sending an authentication request to port 139 or 445.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2018/02/09, Modification date: 2020/03/11

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```
The remote host supports the following SMB dialects :
 _version_  _introduced in windows version_
 2.0.2      Windows 2008
 2.1        Windows 7
 3.0        Windows 8
 3.0.2      Windows 8.1
 3.1.1      Windows 10

The remote host does NOT support the following SMB dialects :
 _version_  _introduced in windows version_
 2.2.2      Windows 8 Beta
 2.2.4      Windows 8 Beta
 3.1        Windows 10
```

125835 - Microsoft Remote Desktop Connection Installed

Synopsis

A graphical interface connection utility is installed on the remote Windows host

Description

Microsoft Remote Desktop Connection (also known as Remote Desktop Protocol or Terminal Services Client) is installed on the remote Windows host.

See Also

http://www.nessus.org/u?1c33f0e7

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2019/06/12, Modification date: 2022/10/10

Ports

10.1.0.141 (TCP/0) Vulnerability State: Resurfaced

```
  Path    : C:\Windows\\System32\\mstsc.exe
  Version : 10.0.26100.7623
```

138603 - Microsoft OneDrive Installed

Synopsis

A file hosting application is installed on the remote host.

Description

Microsoft OneDrive, a file hosting service, is installed on the remote host.

See Also

http://www.nessus.org/u?23c14184

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2020/07/17, Modification date: 2026/01/07

Ports

10.1.0.141 (TCP/445) Vulnerability State: Resurfaced

```
  Path    : C:\Users\Notengo\AppData\Local\Microsoft\OneDrive\
  Version : 26.2.105.1
```

159817 - Windows Credential Guard Status

Synopsis

Retrieves the status of Windows Credential Guard.

Description

Retrieves the status of Windows Credential Guard.
Credential Guard prevents attacks such as such as Pass-the-Hash or Pass-The-Ticket by protecting NTLM password hashes, Kerberos Ticket Granting Tickets, and credentials stored by applications as domain credentials.

See Also

http://www.nessus.org/u?fb8c8c37

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2022/04/18, Modification date: 2023/08/25

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```
Windows Credential Guard is not fully enabled.
The following registry keys have not been set :
  - System\CurrentControlSet\Control\DeviceGuard\RequirePlatformSecurityFeatures : Key not found.
  - System\CurrentControlSet\Control\LSA\LsaCfgFlags : Key not found.
  - System\CurrentControlSet\Control\DeviceGuard\EnableVirtualizationBasedSecurity : Key not
 found.
```

160486 - Server Message Block (SMB) Protocol Version Detection

Synopsis

Verify the version of SMB on the remote host.

Description

The Server Message Block (SMB) Protocol provides shared access to files and printers across nodes on a network.

See Also

http://www.nessus.org/u?f463096b

http://www.nessus.org/u?1a4b3744

Solution

Disable SMB version 1 and block all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

Risk Factor

None

Plugin Information:

Publication date: 2022/05/04, Modification date: 2022/05/04

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```
 - SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\SMB2 : Key not found.
 - SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\SMB3 : Key not found.
 - SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\SMB1 : Key not found.
```

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:

Publication date: 2025/02/26, Modification date: 2025/03/03

Ports

10.1.0.141 (TCP/0) Vulnerability State: Active

```
Following OS Fingerprints were found

Remote operating system : Microsoft Windows Server 2025
```

```
Confidence level : 56
Method : MLSinFP
Type : unknown
Fingerprint : unknown

Remote operating system : Windows 11
Confidence level : 70
Method : Misc
Type : general-purpose
Fingerprint : unknown

Remote operating system : Microsoft Windows 11 Pro Build 26200
Confidence level : 100
Method : SMB_OS
Type : general-purpose
Fingerprint : unknown

Following fingerprints could not be used to determine OS :
 SinFP:!:
   P1:B11113:F0x12:W65535:O0204ffff:M1410:
   P2:B11113:F0x12:W65535:O0204ffff010303080402080affffffff44454144:M1410:
   P3:B00000:F0x00:W0:O0:M0
   P4:191601_7_p=445R
SSLcert:!:i/CN:notengos/CN:notengo
c6b0e3d4b13c8d94c83ce71359570ce86e7338ed
```

10456 - Microsoft Windows SMB Service Enumeration

Synopsis

It is possible to enumerate remote services.

Description

This plugin implements the SvcOpenSCManager() and SvcEnumServices() calls to obtain, using the SMB protocol, the list of active and inactive services of the remote host.
An attacker may use this feature to gain better knowledge of the remote host.

Solution

To prevent the listing of the services from being obtained, you should either have tight login restrictions, so that only trusted users can access your host, and/or you should filter incoming traffic to this port.

Risk Factor

None

References

XREF	IAVT-0001-T-0751

Plugin Information:

Publication date: 2000/07/03, Modification date: 2022/02/01

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```
Active Services :

Application Identity [ AppIDSvc ]
Application Information [ Appinfo ]
AppX Deployment Service (AppXSVC) [ AppXSvc ]
Windows Audio Endpoint Builder [ AudioEndpointBuilder ]
Windows Audio [ Audiosrv ]
Base Filtering Engine [ BFE ]
Background Intelligent Transfer Service [ BITS ]
Background Tasks Infrastructure Service [ BrokerInfrastructure ]
Capability Access Manager Service [ camsvc ]
Connected Devices Platform Service [ CDPSvc ]
Certificate Propagation [ CertPropSvc ]
Client License Service (ClipSVC) [ ClipSVC ]
CoreMessaging [ CoreMessagingRegistrar ]
Cryptographic Services [ CryptSvc ]
DCOM Server Process Launcher [ DcomLaunch ]
DHCP Client [ Dhcp ]
Connected User Experiences and Telemetry [ DiagTrack ]
Display Policy Service [ DispBrokerDesktopSvc ]
Display Enhancement Service [ DisplayEnhancementService ]
DNS Client [ Dnscache ]
Diagnostic Policy Service [ DPS ]
Data Sharing Service [ DsSvc ]
Data Usage [ DusmSvc ]
Windows Event Log [ EventLog ]
COM+ Event System [ EventSystem ]
Windows Font Cache Service [ FontCache ]
Guest Configuration Service [ GCService ]
Group Policy Client [ gpsvc ]
IKE and AuthIP IPsec Keying Modules [ IKEEXT ]
Microsoft Store Install Service [ InstallService ]
Inventory and Compatibility Appraisal service [ InventorySvc ]
IP Helper [ iphlpsvc ]
CNG Key Isolation [ KeyIso ]
Server [ LanmanServer ]
Workstation [ LanmanWorkstation ]
Geolocation Service [ lfsvc ]
Windows License Manager Service [ LicenseManager ]
TCP/IP NetBIOS Helper [ lmhosts ]
Local Session Manager [ LSM ]
Microsoft Defender Core Service [ MDCoreSvc ]
Windows Defender Firewall [ mpssvc ]
Network Connection Broker [ NcbService ]
Network List Service [ netprofm ]
Network Store Interface Service [ nsi ]
Program Compatibility Assistant Service [ PcaSvc ]
Performance Logs & Alerts [ pla ]
Plug and Play [ PlugPlay ]
IPsec Policy Agent [ PolicyAgent ]
Power [ Power ]
User Profile Service [ ProfSvc ]
RdAgent [ RdAgent ]
Remote Registry [ RemoteRegistry ] [...]
```

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:

Publication date: 2002/06/05, Modification date: 2021/02/11

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

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

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:

Publication date: 2003/12/09, Modification date: 2025/06/03

Ports

10.1.0.141 (TCP/0) Vulnerability State: Active

```
Remote operating system : Microsoft Windows 11 Pro Build 26200
Confidence level : 100
Method : SMB_OS

Not all fingerprints could give a match. If you think that these
signatures would help us improve OS fingerprinting, please submit
them by visiting https://www.tenable.com/research/submitsignatures.

SinFP:!:
   P1:B11113:F0x12:W65535:O0204ffff:M1410:
   P2:B11113:F0x12:W65535:O0204ffff010303080402080affffffff44454144:M1410:
   P3:B00000:F0x00:W0:O0:M0
   P4:191601_7_p=445R
SSLcert:!:i/CN:notengos/CN:notengo
c6b0e3d4b13c8d94c83ce71359570ce86e7338ed



The remote host is running Microsoft Windows 11 Pro Build 26200
```

17651 - Microsoft Windows SMB : Obtains the Password Policy

Synopsis

It is possible to retrieve the remote host's password policy using the supplied credentials.

Description

Using the supplied credentials it was possible to extract the password policy for the remote Windows host. The password policy must conform to the Informational System Policy.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2005/03/30, Modification date: 2015/01/12

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```
The following password policy is defined on the remote host:

Minimum password len: 0
Password history len: 0
Maximum password age (d): 60
Password must meet complexity requirements: Enabled
Minimum password age (d): 0
Forced logoff time (s): Not set
Locked account time (s): 600
Time between failed logon (s): 600
Number of invalid logon before locked out (s): 10
```

42897 - SMB Registry : Start the Registry Service during the scan (WMI)

Synopsis

The registry service was enabled for the duration of the scan.

Description

To perform a full credentialed scan, Nessus needs the ability to connect to the remote registry service (RemoteRegistry). If the service is down, this plugin will attempt to start for the duration of the scan.
For this plugin to work, you need to select the option 'Start the Remote Registry service during the scan' on the credentials page when you add your Windows credentials.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2009/11/25, Modification date: 2026/01/20

Ports

10.1.0.141 (TCP/0) Vulnerability State: Active

```
The registry service was successfully started for the duration of the scan.
```

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

Synopsis

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

Description

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

See Also

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

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

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

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2011/12/07, Modification date: 2021/03/09

Ports

10.1.0.141 (TCP/3389) Vulnerability State: Resurfaced

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

  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption
 MAC
    ----------------------        ----------       ---           ----     ---------------------
 ---
    ECDHE-RSA-AES128-SHA256       0xC0, 0x2F       ECDHE         RSA      AES-GCM(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x30       ECDHE         RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDHE         RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDHE         RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDHE         RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDHE         RSA      AES-CBC(256)
 SHA384

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

77668 - Windows Prefetch Folder

Synopsis

Nessus was able to retrieve the Windows prefetch folder file list.

Description

Nessus was able to retrieve and display the contents of the Windows prefetch folder (%systemroot%\prefetch\*). This information shows programs that have run with the prefetch and superfetch mechanisms enabled.

See Also

http://www.nessus.org/u?8242d04f

http://www.nessus.org/u?d6b15983

http://www.forensicswiki.org/wiki/Prefetch

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2014/09/12, Modification date: 2018/11/15

Ports

10.1.0.141 (TCP/0) Vulnerability State: Resurfaced

```
 + HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters
rootdirpath :
enableprefetcher : 3

+ Prefetch file list :
  - \Windows\prefetch\AM_DELTA.EXE-3A6EE7FD.pf
  - \Windows\prefetch\AM_DELTA_PATCH_1.443.846.0.EX-3243FFBB.pf
  - \Windows\prefetch\AM_DELTA_PATCH_1.443.965.0.EX-35F75E45.pf
  - \Windows\prefetch\AM_DELTA_PATCH_1.443.967.0.EX-37F67CAF.pf
  - \Windows\prefetch\AM_DELTA_PATCH_1.443.983.0.EX-E141E4B5.pf
  - \Windows\prefetch\AM_DELTA_PATCH_1.443.993.0.EX-B7E6B722.pf
  - \Windows\prefetch\APPACTIONS.EXE-43383A22.pf
  - \Windows\prefetch\APPLICATIONFRAMEHOST.EXE-4CE44C83.pf
  - \Windows\prefetch\ARP.EXE-AE6635A1.pf
  - \Windows\prefetch\ATBROKER.EXE-8B8F7F7C.pf
  - \Windows\prefetch\AUDIODG.EXE-9848A323.pf
  - \Windows\prefetch\AUDITPOL.EXE-5C071DAC.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-09AB7D2E.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-140EC32A.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-27DD6AFB.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-637E22DB.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-714649B0.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-77A150F6.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-8E5D029A.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-A57C77B3.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-A877F937.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-AE3EC8B2.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-B1940266.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-CA0D9CCE.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-CE1F4D27.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-D0E06976.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-E04F3FAC.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-E34F3B7C.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-ECC08AAF.pf
  - \Windows\prefetch\BACKGROUNDTASKHOST.EXE-ECD24DAC.pf
  - \Windows\prefetch\BACKGROUNDTRANSFERHOST.EXE-2046E6BC.pf
  - \Windows\prefetch\BACKGROUNDTRANSFERHOST.EXE-52575DB6.pf
  - \Windows\prefetch\BACKGROUNDTRANSFERHOST.EXE-B02625C4.pf
  - \Windows\prefetch\BACKGROUNDTRANSFERHOST.EXE-BBDBFF65.pf
 [...]
```

117887 - OS Security Patch Assessment Available

Synopsis

Nessus was able to log in to the remote host using the provided credentials and enumerate OS security patch levels.

Description

Nessus was able to determine OS security patch levels by logging into the remote host and running commands to determine the version of the operating system and its components. The remote host was identified as an operating system or device that Nessus supports for patch and update assessment. The necessary information was obtained to perform these checks.

Solution

N/A

Risk Factor

None

References

XREF	IAVB-0001-B-0516

Plugin Information:

Publication date: 2018/10/02, Modification date: 2021/07/12

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```
OS Security Patch Assessment is available.

Account  : 10.1.0.141\Notengo
Protocol : SMB
```

126527 - Microsoft Windows SAM user enumeration

Synopsis

Nessus was able to enumerate domain users from the local SAM.

Description

Using the domain security identifier (SID), Nessus was able to enumerate the domain users on the remote Windows system using the Security Accounts Manager.
Note: Unable to obtain SMB SAMR user data during Agent scans.
Rendering User data obtained by plugin 171956

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2019/07/08, Modification date: 2025/06/04

Ports

10.1.0.141 (TCP/0) Vulnerability State: Resurfaced

```
  - Administrator (id S-1-5-21-1658136452-1347933459-1000, Administrator)
  - DefaultAccount (id S-1-5-21-1658136452-1347933459-503, A user account managed by the system.)
  - DisabledGuest_01 (id S-1-5-21-1658136452-1347933459-501, Guest account, Built-in account for
 guest access to the computer/domain)
  - Notengo (id S-1-5-21-1658136452-1347933459-500, Built-in account for administering the
 computer/domain, Administrator account)
  - WDAGUtilityAccount (id S-1-5-21-1658136452-1347933459-504, A user account managed and used by
 the system for Windows Defender Application Guard scenarios.)
```

151440 - Microsoft Windows Print Spooler Service Enabled

Synopsis

The Microsoft Windows Print Spooler service on the remote host is enabled.

Description

The Microsoft Windows Print Spooler service (spoolsv.exe) on the remote host is enabled.

See Also

http://www.nessus.org/u?8fc5df24

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2021/07/07, Modification date: 2021/07/07

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```
The Microsoft Windows Print Spooler service on the remote host is enabled.
```

156899 - SSL/TLS Recommended Cipher Suites

Synopsis

The remote host advertises discouraged SSL/TLS ciphers.

Description

The remote host has open SSL/TLS ports which advertise discouraged cipher suites. It is recommended to only enable support for the following cipher suites:
TLSv1.3:
- 0x13,0x01 TLS13_AES_128_GCM_SHA256
- 0x13,0x02 TLS13_AES_256_GCM_SHA384
- 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256
TLSv1.2:
- 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256
- 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256
- 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384
- 0xC0,0x30 ECDHE-RSA-AES256-GCM-SHA384
- 0xCC,0xA9 ECDHE-ECDSA-CHACHA20-POLY1305
- 0xCC,0xA8 ECDHE-RSA-CHACHA20-POLY1305
This is the recommended configuration for the vast majority of services, as it is highly secure and compatible with nearly every client released in the last five (or more) years.

See Also

https://wiki.mozilla.org/Security/Server_Side_TLS

https://ssl-config.mozilla.org/

Solution

Only enable support for recommened cipher suites.

Risk Factor

None

Plugin Information:

Publication date: 2022/01/20, Modification date: 2024/02/12

Ports

10.1.0.141 (TCP/3389) Vulnerability State: Resurfaced

```
The remote host has listening SSL/TLS ports which advertise the discouraged cipher suites outlined
 below:


  High Strength Ciphers (>= 112-bit key)

    Name                          Code             KEX           Auth     Encryption
 MAC
    ----------------------        ----------       ---           ----     ---------------------
 ---
    RSA-AES128-SHA256             0x00, 0x9C       RSA           RSA      AES-GCM(128)
 SHA256
    RSA-AES256-SHA384             0x00, 0x9D       RSA           RSA      AES-GCM(256)
 SHA384
    ECDHE-RSA-AES128-SHA          0xC0, 0x13       ECDHE         RSA      AES-CBC(128)
 SHA1
    ECDHE-RSA-AES256-SHA          0xC0, 0x14       ECDHE         RSA      AES-CBC(256)
 SHA1
```

```
    AES128-SHA                    0x00, 0x2F       RSA           RSA      AES-CBC(128)
 SHA1
    AES256-SHA                    0x00, 0x35       RSA           RSA      AES-CBC(256)
 SHA1
    ECDHE-RSA-AES128-SHA256       0xC0, 0x27       ECDHE         RSA      AES-CBC(128)
 SHA256
    ECDHE-RSA-AES256-SHA384       0xC0, 0x28       ECDHE         RSA      AES-CBC(256)
 SHA384
    RSA-AES128-SHA256             0x00, 0x3C       RSA           RSA      AES-CBC(128)
 SHA256
    RSA-AES256-SHA256             0x00, 0x3D       RSA           RSA      AES-CBC(256)
 SHA256

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

161691 - The Microsoft Windows Support Diagnostic Tool (MSDT) RCE Workaround Detection (CVE-2022-30190)

Synopsis

Checks for the HKEY_CLASSES_ROOT\ms-msdt registry key.

Description

The remote host has the HKEY_CLASSES_ROOT\ms-msdt registry key. This is a known exposure for CVE-2022-30190.
Note that Nessus has not tested for CVE-2022-30190. It is only checking if the registry key exists. The recommendation is to apply the latest patch.

See Also

http://www.nessus.org/u?440e4ba1

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190

http://www.nessus.org/u?b9345997

Solution

Apply the latest Cumulative Update.

Risk Factor

None

Plugin Information:

Publication date: 2022/05/31, Modification date: 2022/07/28

Ports

10.1.0.141 (TCP/445) Vulnerability State: Resurfaced

```
The HKEY_CLASSES_ROOT\ms-msdt registry key exists on the target. This may indicate that the target
 is vulnerable to CVE-2022-30190, if the vendor patch is not applied.
```

166555 - WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)

Synopsis

The remote Windows host is potentially missing a mitigation for a remote code execution vulnerability.

Description

The remote system may be in a vulnerable state to CVE-2013-3900 due to a missing or misconfigured registry keys:
- HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config
\EnableCertPaddingCheck An unauthenticated, remote attacker could exploit this, by sending specially crafted requests, to execute arbitrary code on an affected host.

See Also

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900 http://www.nessus.org/u?9780b9d2

Solution

Add and enable registry value EnableCertPaddingCheck:
- HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck
Additionally, on 64 Bit OS systems, Add and enable registry value EnableCertPaddingCheck:
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck

Risk Factor

High

Vulnerability Priority Rating (VPR)

9.0

CVSS v3.0 Base Score

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

CVSS v3.0 Temporal Score

8.4 (E:H/RL:O/RC:C)

CVSS Base Score

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

CVSS Temporal Score

6.6 (E:H/RL:OF/RC:C)

STIG Severity

II

References

CVE	CVE-2013-3900
XREF	CISA-KNOWN-EXPLOITED-2022/07/10
XREF	IAVA-2013-A-0227

Plugin Information:

Publication date: 2022/10/26, Modification date: 2025/12/17

Ports

10.1.0.141 (TCP/445) Vulnerability State: Resurfaced

```
Nessus detected the following potentially insecure registry key configuration:
   - Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck is not present in the
registry.
   - Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck is not
present in the registry.
```

176212 - Microsoft Edge Add-on Enumeration (Windows)

Synopsis

One or more Microsoft Edge browser extensions are installed on the remote host.

Description

Nessus was able to enumerate Microsoft Edge browser extensions installed on the remote host.

See Also

https://microsoftedge.microsoft.com/addons

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2023/05/22, Modification date: 2026/02/03

Ports

10.1.0.141 (TCP/445) Vulnerability State: Resurfaced

```
User : Notengo
|- Browser : Edge
  |- Add-on information :

    Name        : Google Docs Offline
    Description : Edit, create, and view your documents, spreadsheets, and presentations — all
 without internet access.
    Version     : 1.100.1
    Path        : C:\Users\Notengo\AppData\Local\Microsoft\Edge\User Data\Default\Extensions
\ghbmnnjooekpmoecnnnilnnbdlolhkhi\1.100.1_0

    Name        : Edge relevant text changes
    Description : Edge relevant text changes on select websites to improve user experience and
 precisely surfaces the action they want to take.
    Version     : 1.2.1
    Update Date : Feb.  5, 2026 at 06:27:47 GMT
    Path        : C:\Users\Notengo\AppData\Local\Microsoft\Edge\User Data\Default\Extensions
\jmjflgjpcpepeafmmgdpfkogkghcpiha\1.2.1_0
```

10863 - SSL Certificate Information

Synopsis

This plugin displays the SSL certificate.

Description

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

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2008/05/19, Modification date: 2021/02/03

Ports

10.1.0.141 (TCP/3389) Vulnerability State: Active

```
 Subject Name:

Common Name: notengo

Issuer Name:

Common Name: notengo

Serial Number: 4B 17 CD 0A 47 90 6C 9A 4B 23 FD FA 3D 2C 43 00

Version: 3

Signature Algorithm: SHA-256 With RSA Encryption

Not Valid Before: Jan 21 05:47:21 2026 GMT
Not Valid After: Jul 23 05:47:21 2026 GMT

Public Key Info:

Algorithm: RSA Encryption
Key Length: 2048 bits
Public Key: 00 E6 CB BF 25 42 0F BB 92 EA B7 42 56 C9 F2 44 55 52 4C 96
            B5 B7 B5 5B 3B F3 3C B3 24 89 0F AE 1E C9 7E DF 59 A0 56 26
            82 C8 86 F3 73 00 D4 EF 32 17 90 0D 96 A2 FE 6C B3 29 67 E5
            59 EB 5B 94 F8 FD C8 BA 07 E3 4A 8A 09 A4 AD 62 F0 8C 17 C2
            9C CD 6D D9 A8 DC 26 59 67 81 0E 05 9C 31 0B 6F 32 B2 65 07
            55 03 F4 9B 59 F7 62 D3 C9 45 45 84 35 0B 7E AB 6D 44 59 1A
            ED 84 0C AA 45 5E 5D 71 78 D1 EB 6B 29 C9 A3 38 31 9D F2 E1
            9E D0 F8 0C 8C 84 87 10 EF AC A2 FE A3 1F B0 53 75 26 CB 98
            56 0E 47 D5 5A 01 7C 23 27 96 5F 12 DE 76 89 FB A7 CD 88 6D
            41 F4 36 95 03 53 23 53 43 AA 74 8A CC 9C 48 BE 2F AB AD B9
            D7 E6 2B B7 CB 23 A1 E9 48 BE 9C 3A 8B C9 C2 48 AB 9A 78 2B
            B0 E1 C3 1A 4A 1A E1 28 36 61 90 14 8F 90 60 CA EE 3A 09 2B
            36 54 C7 07 CF 81 CD 17 AB C6 E8 2E 0D 10 10 3B 21
Exponent: 01 00 01

Signature Length: 256 bytes / 2048 bits
Signature: 00 42 C7 85 33 4E 0C CD 08 D6 07 80 7B 73 BE A5 68 BE 8F 95
           36 37 F8 F7 E5 B2 75 A0 E7 31 73 D7 C8 EA 6E F0 D0 60 F6 8B
           E9 68 4D A4 1C 5E 57 94 CA E4 F8 80 0F 7A E4 23 5A 31 26 CD
           A2 D3 3A 7F 31 CC B4 13 F9 65 88 D6 EA EB 9D 01 FA 16 7E 64
           B2 43 2F BE 3E AA 78 3E A4 B3 BB 43 89 CE 66 95 AC BC BF 4D
           75 3D 9B DD 19 38 C0 A9 A9 BE 37 85 E5 FB E7 93 B7 C2 04 75
           53 28 95 13 F9 BA CB 14 2F F6 0B 4C 53 00 AF 53 D1 B7 58 CC
           D2 2F 15 4F 3E 37 68 07 FF 93 9E 98 39 D0 E4 F5 44 AB FA 2F
           30 1F A8 50 B4 3E D2 9D 83 8D D5 09 86 6E 3E D9 87 C6 1F B0
           F6 66 8B 87 63 50 66 9A B5 A7 E2 [...]
```

161502 - Microsoft Windows Logged On Users

Synopsis

Nessus was able to determine the logged on users from the registry

Description

Using the HKU registry, Nessus was able to enumerate the SIDs of logged on users

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2022/05/25, Modification date: 2025/10/01

Ports

10.1.0.141 (TCP/445) Vulnerability State: Resurfaced

```
Logged on users :
  - S-1-5-21-1658136452-1347933459-2279167012-500
    Domain   : notengo
    Username : Notengo
```

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:

Publication date: 2011/05/23, Modification date: 2025/03/12

Ports

10.1.0.141 (TCP/0) Vulnerability State: Active

```
Remote device type : general-purpose
Confidence level : 100
```

159929 - Windows LSA Protection Status

Synopsis

Windows LSA Protection is disabled on the remote Windows host.

Description

The LSA Protection validates users for local and remote sign-ins and enforces local security policies to prevent reading memory and code injection by non-protected processes. This provides added security for the credentials that the LSA stores and manages. This protects against Pass-the-Hash or Mimikatz-style attacks.

Solution

Enable LSA Protection per your corporate security guidelines.

Risk Factor

None

Plugin Information:

Publication date: 2022/04/20, Modification date: 2025/06/16

Ports

10.1.0.141 (TCP/445) Vulnerability State: Active

```
LSA Protection is enabled (without UEFI).
```

92369 - Microsoft Windows Time Zone Information

Synopsis

Nessus was able to collect and report time zone information from the remote host.

Description

Nessus was able to collect time zone information from the remote Windows host and generate a report as a CSV attachment.

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2023/06/06

Ports

10.1.0.141 (TCP/0) Vulnerability State: Resurfaced

```
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\TimeZoneKeyName : UTC
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\StandardName : @tzres.dll,-932
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DaylightName : @tzres.dll,-931
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DynamicDaylightTimeDisabled : 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\StandardBias : 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DaylightBias : 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\Bias : 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\DaylightStart :
 00000000000000000000000000000000
HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\StandardStart :
 00000000000000000000000000000000
```

92429 - Recycle Bin Files

Synopsis

Nessus was able to enumerate files in the recycle bin on the remote host.

Description

Nessus was able to generate a list of all files found in $Recycle.Bin subdirectories.

See Also

http://www.nessus.org/u?0c1a03df

http://www.nessus.org/u?61293b38

Solution

N/A

Risk Factor

None

Plugin Information:

Publication date: 2016/07/19, Modification date: 2018/11/15

Ports

10.1.0.141 (TCP/0) Vulnerability State: Resurfaced

```
C:\\$Recycle.Bin\\.
C:\\$Recycle.Bin\\..
C:\\$Recycle.Bin\\S-1-5-18
C:\\$Recycle.Bin\\S-1-5-21-1058185559-3351018384-2725476567-500
C:\\$Recycle.Bin\\S-1-5-21-1658136452-1347933459-2279167012-500
C:\\$Recycle.Bin\\S-1-5-18\.
C:\\$Recycle.Bin\\S-1-5-18\..
C:\\$Recycle.Bin\\S-1-5-18\desktop.ini
C:\\$Recycle.Bin\\S-1-5-21-1058185559-3351018384-2725476567-500\.
C:\\$Recycle.Bin\\S-1-5-21-1058185559-3351018384-2725476567-500\..
C:\\$Recycle.Bin\\S-1-5-21-1058185559-3351018384-2725476567-500\desktop.ini
C:\\$Recycle.Bin\\S-1-5-21-1658136452-1347933459-2279167012-500\.
C:\\$Recycle.Bin\\S-1-5-21-1658136452-1347933459-2279167012-500\..
C:\\$Recycle.Bin\\S-1-5-21-1658136452-1347933459-2279167012-500\desktop.ini
```

Assets Summary (Executive)

10.1.0.141

Summary

Critical	High	Medium	Low	Info	Total
0	1	4	0	94	99

Details

Severity	Plugin Id	Name
High	166555	WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)
Medium	104743	TLS Version 1.0 Protocol Detection
Medium	57582	SSL Self-Signed Certificate
Medium	157288	TLS Version 1.1 Deprecated Protocol
Medium	51192	SSL Certificate Cannot Be Trusted
Info	160576	Windows Services Registry ACL
Info	125835	Microsoft Remote Desktop Connection Installed
Info	45590	Common Platform Enumeration (CPE)
Info	72367	Microsoft Internet Explorer Version Detection
Info	92426	OpenSaveMRU History
Info	51351	Microsoft .NET Framework Detection
Info	58452	Microsoft Windows Startup Software Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	34097	BIOS Info (SMB)
Info	11457	Microsoft Windows SMB Registry : Winlogon Cached Password Weakness
Info	159817	Windows Credential Guard Status
Info	42897	SMB Registry : Start the Registry Service during the scan (WMI)
Info	117885	Target Credential Issues by Authentication Protocol - Intermittent Authentication Failure
Info	136318	TLS Version 1.2 Protocol Detection
Info	57033	Microsoft Patch Bulletin Feasibility Check
Info	66424	Microsoft Malicious Software Removal Tool Installed
Info	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
Info	21643	SSL Cipher Suites Supported
Info	42898	SMB Registry : Stop the Registry Service after the scan (WMI)
Info	77668	Windows Prefetch Folder

Info	93962	Microsoft Security Rollup Enumeration
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	187318	Microsoft Windows Installed
Info	10456	Microsoft Windows SMB Service Enumeration
Info	92368	Microsoft Windows Scripting Host Settings
Info	160486	Server Message Block (SMB) Protocol Version Detection
Info	10863	SSL Certificate Information
Info	162560	Microsoft Internet Explorer Installed
Info	176212	Microsoft Edge Add-on Enumeration (Windows)
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
Info	10902	Microsoft Windows 'Administrators' Group User List
Info	10396	Microsoft Windows SMB Shares Access
Info	135860	WMI Not Available
Info	92364	Microsoft Windows Environment Variables
Info	11011	Microsoft Windows SMB Service Detection
Info	148541	Windows Language Settings Detection
Info	138603	Microsoft OneDrive Installed
Info	103871	Microsoft Windows Network Adapters
Info	126527	Microsoft Windows SAM user enumeration
Info	38689	Microsoft Windows SMB Last Logged On User Disclosure
Info	10400	Microsoft Windows SMB Registry Remotely Accessible
Info	178102	Microsoft Windows Installed Software Version Enumeration
Info	121010	TLS Version 1.1 Protocol Detection
Info	64814	Terminal Services Use SSL/TLS
Info	162174	Windows Always Installed Elevated Status
Info	131023	Windows Defender Installed
Info	161691	The Microsoft Windows Support Diagnostic Tool (MSDT) RCE Workaround Detection (CVE-2022-30190)
Info	58181	Windows DNS Server Enumeration
Info	92369	Microsoft Windows Time Zone Information
Info	44401	Microsoft Windows SMB Service Config Enumeration

Info	62042	SMB QuickFixEngineering (QFE) Enumeration
Info	92429	Recycle Bin Files
Info	156899	SSL/TLS Recommended Cipher Suites
Info	56984	SSL / TLS Versions Supported
Info	54615	Device Type
Info	117887	OS Security Patch Assessment Available
Info	92424	MUICache Program Execution History
Info	25220	TCP/IP Timestamps Supported
Info	20811	Microsoft Windows Installed Software Enumeration (credentialed check)
Info	277650	Remote Services Not Using Post-Quantum Ciphers
Info	11936	OS Identification
Info	161502	Microsoft Windows Logged On Users
Info	92365	Microsoft Windows Hosts File
Info	63080	Microsoft Windows Mounted Devices
Info	209654	OS Fingerprints Detected
Info	200493	Microsoft Windows Start Menu Software Version Enumeration
Info	10335	Nessus TCP scanner
Info	10287	Traceroute Information
Info	10940	Remote Desktop Protocol Service Detection
Info	136969	Microsoft Edge Chromium Installed
Info	92435	UserAssist Execution History
Info	160301	Link-Local Multicast Name Resolution (LLMNR) Service Detection
Info	17651	Microsoft Windows SMB : Obtains the Password Policy
Info	92431	User Shell Folders Settings
Info	16193	Antivirus Software Check
Info	280146	Microsoft Azure Guest Agent Installed (Windows)
Info	48763	Microsoft Windows 'CWDIllegalInDllSearch' Registry Setting
Info	19506	Nessus Scan Information
Info	277654	TLS Supported Groups
Info	138330	TLS Version 1.3 Protocol Detection
Info	92434	User Download Folder Files

Info	48942	Microsoft Windows SMB Registry : OS Version and Processor Architecture
Info	10395	Microsoft Windows SMB Shares Enumeration
Info	10394	Microsoft Windows SMB Log In Possible
Info	141118	Target Credential Status by Authentication Protocol - Valid Credentials Provided
Info	92421	Internet Explorer Typed URLs
Info	100871	Microsoft Windows SMB Versions Supported (remote check)
Info	159929	Windows LSA Protection Status
Info	92428	Recent File History
Info	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	92415	Application Compatibility Cache
Info	151440	Microsoft Windows Print Spooler Service Enabled