TRIPWIRE® IP360

TECHNICAL ANALYSIS

Tue September 3, 2024

Networks

A_AHS_Scan2_NoSIH

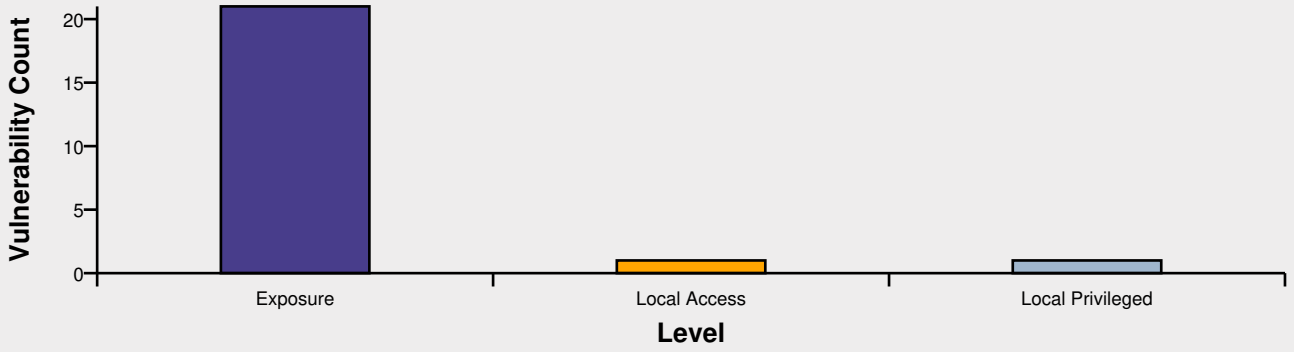
Filters

Windows OS Only

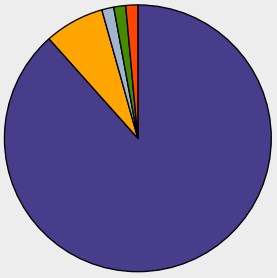
Report Summary

Networks/Network Groups	A_AHS_Scan2_NoSIH	**Filters**	Windows OS Only
Hosts	1	**Asset Value**	0
Average Host Score	6	**Vulnerabilities**	24
Applications/Services	70		

Vulnerability Level Distribution

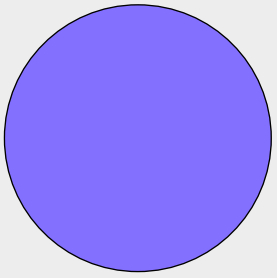


Service Distribution



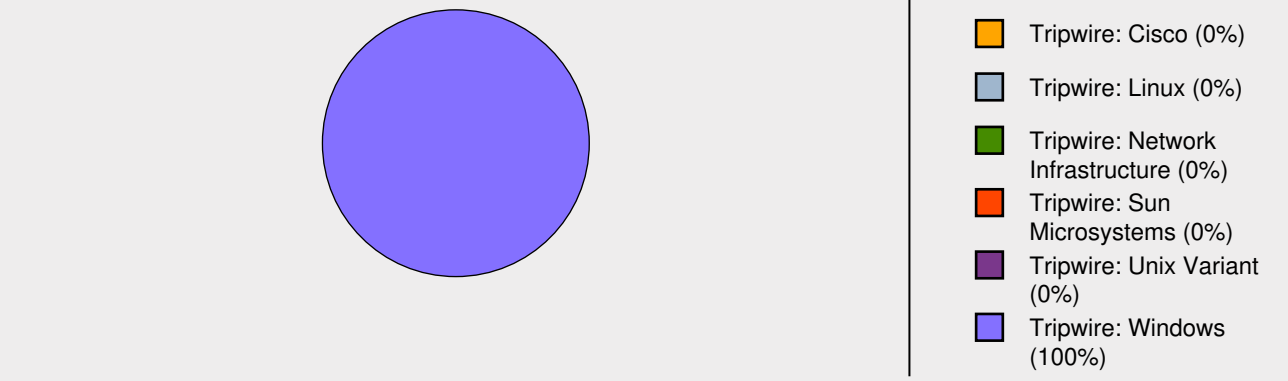
- Multi-Port Protocol (88%)
- Other (7%)
- NetBIOS Name Service (1%)
- Direct SMB Hosting Service (1%)
- NetBIOS Session Service (1%)

OS Distribution by OS Group

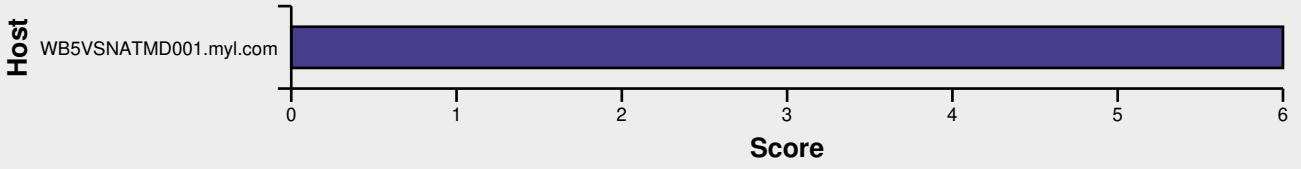


- Mac OS (0%)
- Tripwire: Cisco (0%)
- Tripwire: Linux (0%)
- Tripwire: Network Infrastructure (0%)
- Tripwire: Sun Microsystems (0%)
- Tripwire: Unix Variant (0%)
- Tripwire: Windows (100%)

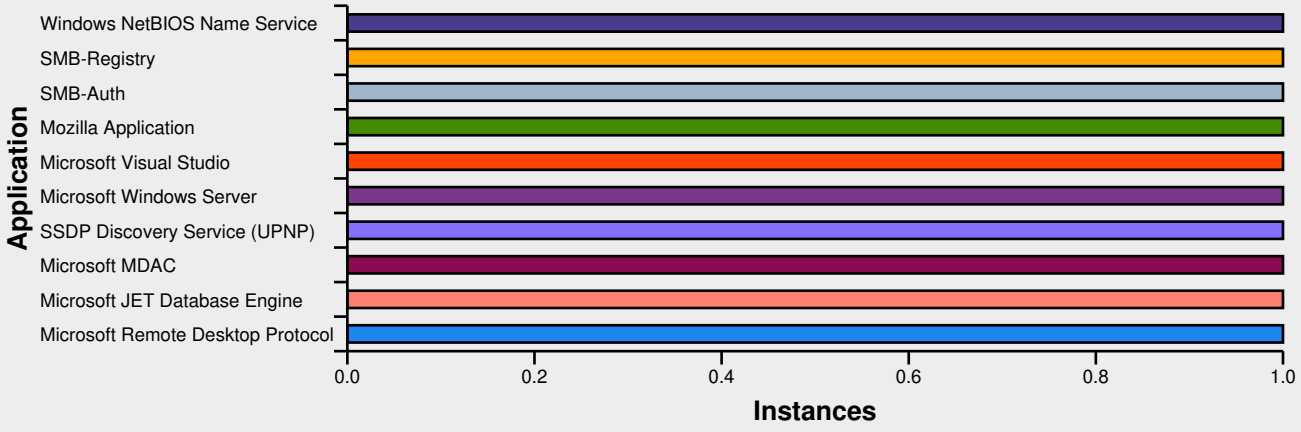
Vuln Distribution by OS Group

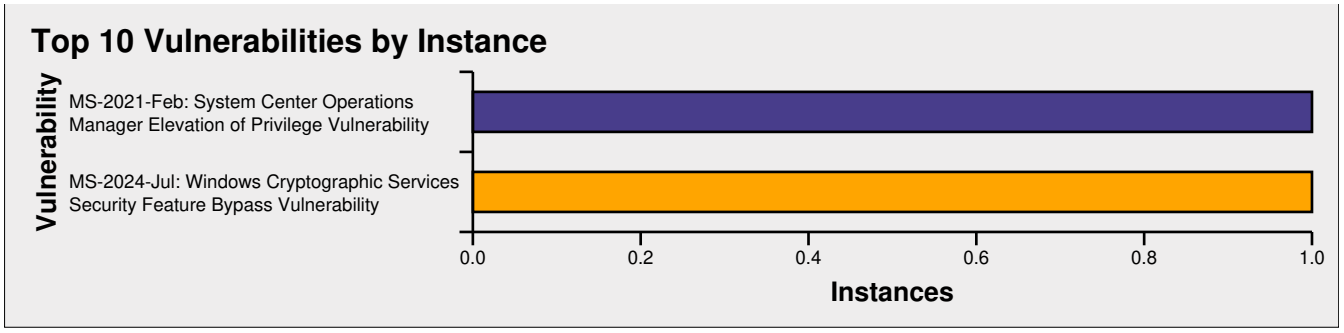


Top 10 Most Vulnerable Hosts



Top 10 Applications by Instance




Top 10 Vulnerabilities by Instance
Vulnerability
MS-2021-Feb: System Center Operations Manager Elevation of Privilege Vulnerability
MS-2024-Jul: Windows Cryptographic Services Security Feature Bypass Vulnerability
0.0
0.2
0.4
0.6
0.8
1.0
Instances

Hosts

Hostname	IP Address	OS	Agent	Owner	Asset Value	Score
WB5VSNATMD0	10.250.132.106	Windows Server 2022	No	None	0	6

Host Summary

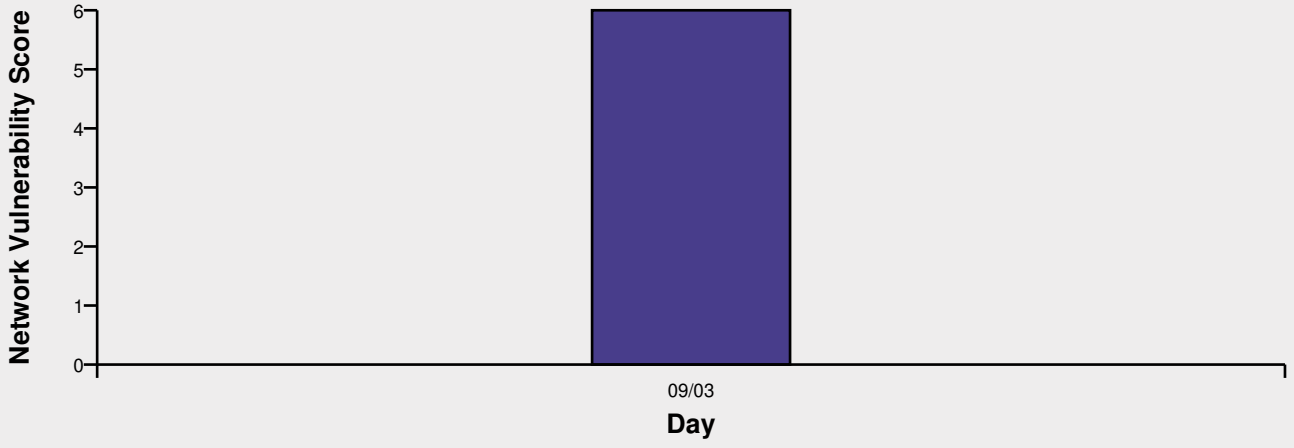
Hostname	WB5VSNATMD001.myl.com	**IP Address**	10.250.132.106
Score	6	**Asset Value**	0
OS Name	Windows Server 2022	**Owner**	None
NetBIOS Name	WB5VSNATMD001	**Mac Address (NetBIOS)**	
Domain/Workgroup	MYL		

Operating System

OS Name
Windows Server 2022

Vulnerability Distribution by Level

Score Distribution by Day



Host Share List

NetBIOS Share
ADMIN$

continued on next page

NetBIOS Share
C$
D$
IPC$
P$

Vulnerabilities

Vulnerability	CVE	# of Ports	Score
MS-2021-Feb: System Center Operations Manager Elevation of Privilege Vulnerability	CVE-2021-1728	1	6
NetBIOS SSN Available		1	0
SMB AUTHENTICATION SUCCESS		1	0
Host has IPv6 Enabled		1	0
RPC DCOM AUTHENTICATION SUCCESS		1	0
WMI AUTHENTICATION SUCCESS		1	0
The contents of an SMB share may be enumerated		1	0
A Windows SMB share permits read access to Everyone [via SMB]		1	0
Microsoft Remote Desktop Service Available		1	0
IP Addresses Enumerated Via NetBIOS		1	0
Portable Storage Devices Detected (Windows)		1	0
BigFix		1	0
No UNC Paths Configured for Integrity		1	0
No UNC Paths Configured for Privacy		1	0
No UNC Paths Configured for Mutual Authentication		1	0
Windows DRT Command Success		1	0
MS15-124: Microsoft Browser ASLR Bypass Vulnerability	CVE-2015-6161	1	0
CredSSP "AllowEncryptionOracle" Policy Setting: Mitigated Mode		1	0
CACHED APPLICATION DATA		1	0
ms-msdt Protocol Scheme Configured		1	0
search-ms Protocol Scheme Configured		1	0
Unquoted Service Path Weakness		1	0
DCE RPC mapper available		1	0
MS-2024-Jul: Windows Cryptographic Services Security Feature Bypass Vulnerability	CVE-2024-30098	1	0

Applications

Service	Application	Port
DCE/MS RPC over TCP	DCE/MS RPC Endpoint Mapper Interface (TCP)	135
Direct SMB Hosting Service	Microsoft Windows OS Family 21H2 Direct SMB Session Service	445
IPv4 Layer 4		0
Microsoft Remote Desktop Protocol		3389
Multi-Port Protocol	AllJoyn Router Service	0
Multi-Port Protocol	CNG Key Isolation Service	0
Multi-Port Protocol	DirectWrite	0
Multi-Port Protocol	DirectX 10.x	0
Multi-Port Protocol	DirectX 11.x	0

continued on next page

Service	Application	Port
Multi-Port Protocol	DirectX 12.x	0
Multi-Port Protocol	DirectX 9.0c	0
Multi-Port Protocol	HCL BigFix Client 10.0.7.52	0
Multi-Port Protocol	Host has IPv6 Enabled	0
Multi-Port Protocol	HTTP Service	0
Multi-Port Protocol	IKE and AuthIP IPsec Keying Modules Service	0
Multi-Port Protocol	Ink Support Feature	0
Multi-Port Protocol	IPSec Policy Agent Service	0
Multi-Port Protocol	Microsoft .NET Framework v4.8.x	0
Multi-Port Protocol	Microsoft Cryptographic Services	0
Multi-Port Protocol	Microsoft Internet Explorer 11	0
Multi-Port Protocol	Microsoft JET Database Engine	0
Multi-Port Protocol	Microsoft JScript	0
Multi-Port Protocol	Microsoft Korean Language IME	0
Multi-Port Protocol	Microsoft MDAC	0
Multi-Port Protocol	Microsoft Paint	0
Multi-Port Protocol	Microsoft Remote Desktop Protocol 10.0	0
Multi-Port Protocol	Microsoft SharePoint	0
Multi-Port Protocol	Microsoft SoftGrid/Application Virtualization	0
Multi-Port Protocol	Microsoft System Center Operations Monitoring Agent 2019	0
Multi-Port Protocol	Microsoft Terminal Services Client	0
Multi-Port Protocol	Microsoft VBScript	0
Multi-Port Protocol	Microsoft Visual Studio	0
Multi-Port Protocol	Microsoft Windows Server	0
Multi-Port Protocol	Microsoft Windows Telnet Client	0
Multi-Port Protocol	Mozilla Application	0
Multi-Port Protocol	MPEG Layer-3 codecs	0
Multi-Port Protocol	MSXML 3.0	0
Multi-Port Protocol	MSXML 6.0	0
Multi-Port Protocol	Print Spooler Service	0
Multi-Port Protocol	Remote Registry Service	0
Multi-Port Protocol	Smart Card Service	0
Multi-Port Protocol	SSDP Discovery Service (UPNP)	0
Multi-Port Protocol	Symantec AntiVirus	0
Multi-Port Protocol	Symantec Endpoint Protection Client	0
Multi-Port Protocol	Telephony Service	0
Multi-Port Protocol	USB Attached SCSI Protocol Service	0
Multi-Port Protocol	VMware Tools 12.x	0
Multi-Port Protocol	Volume Shadow Copy Service	0
Multi-Port Protocol	Windows Address Book	0
Multi-Port Protocol	Windows ATL Component	0
Multi-Port Protocol	Windows CloudExperienceHost Broker	0
Multi-Port Protocol	Windows Domain Joined Host	0
Multi-Port Protocol	Windows Mail	0
Multi-Port Protocol	Windows Media Player 12	0
Multi-Port Protocol	Windows OpenSSH Client	0
Multi-Port Protocol	Windows OS (Not Server Core)	0
Multi-Port Protocol	Windows Projected File System	0
Multi-Port Protocol	Windows Remote Access Connection Manager	0

continued on next page

Service	Application	Port
Multi-Port Protocol	Windows Remote Desktop Available	0
Multi-Port Protocol	Windows Script Host	0
Multi-Port Protocol	Windows Search / Windows Desktop Search	0
Multi-Port Protocol	Windows Secure Boot Enabled	0
Multi-Port Protocol	Windows Server 2022	0
Multi-Port Protocol	Windows Workstation Service	0
Multi-Port Protocol	WordPad	0
NetBIOS Name Service	Windows NetBIOS Name Service	137
NetBIOS Session Service	Microsoft Windows OS Family 21H2 NetBIOS Session Service	139
Open TCP Port	N/A	1556
SMB-Auth	N/A	0
SMB-Registry	N/A	0

Configuration Checks

Configuration Check	Discovery Method	Value
All Hardened UNC Paths Found	WDRT	{}
AllowEncryptionOracle	WDRT	AllowEncryptionOracle is not set.
Automatic Updates Enabled	WDRT	Windows version does not support Automatic Updates
DNS Computer Name	TCP	TCP(139): WB5VSNATMD001.myl.com, TCP(445): WB5VSNATMD001.myl.com
DNS Domain Name	TCP	TCP(139): myl.com, TCP(445): myl.com
DNS Tree Name	TCP	TCP(139): myl.com, TCP(445): myl.com
IP Addresses via NETBIOS	UDP	10.250.132.106
Last Logged In User	WDRT	MYL\svc_automation
Netbios Computer Name	TCP	TCP(139): WB5VSNATMD001, TCP(445): WB5VSNATMD001
Netbios Domain Name	TCP	TCP(139): MYL, TCP(445): MYL
Nmap OS String	TCP	
Nmap Status	NMAP	Global: Nmap Not Configured
SMB Shares Everyone File System Read Access	SMB	D$, P$
SMB Shares Where Contents May Be Enumerated	SMB	ADMIN$, C$, D$, P$
SMB Username	SMB	myl\\svc_ncirclecred
SSL Certificate Extended Key Usage	SSL	TCP(3389): serverAuth
SSL Certificate Issuer	SSL	TCP(3389): commonName=WB5VSNATMD001.myl.com
SSL Certificate Key Usage	SSL	TCP(3389): keyEncipherment dataEncipherment
SSL Certificate MD5 Thumbprint	SSL	TCP(3389): 90:BE:47:25:4F:83:9C:0E:E0:C4:8F:FE:F5:4D:34:B6
SSL Certificate Public Key Size	SSL	TCP(3389): 2048 bits
SSL Certificate SHA1 Thumbprint	SSL	TCP(3389): 95:3E:3D:10:C6:DD:35:7A:84:C2:DC:E0:35:62:3E:5E:7F:38:78:D3
SSL Certificate Serial Number	SSL	TCP(3389): 10:72:19:D4:BA:42:05:86:4D:C7:3C:FE:32:9A:9E:DB

continued on next page

Configuration Check	Discovery Method	Value
SSL Certificate Signature Algorithm	SSL	TCP(3389): sha256WithRSAEncryption
SSL Certificate Subject	SSL	TCP(3389): commonName=WB5VSNATMD001.myl.com
SSL Certificate Valid From	SSL	TCP(3389): Mon Sep 2 07:08:02 2024 UTC
SSL Certificate Valid To	SSL	TCP(3389): Tue Mar 4 07:08:02 2025 UTC
SSL/TLS Enabled Ciphers	SSL	TCP(3389) TLSv1.2: TLS_RSA_WITH_AES_256_GCM_SHA384\, TLS_RSA_WITH_AES_128_GCM_SHA256\, TLS_RSA_WITH_AES_256_CBC_SHA256\, TLS_RSA_WITH_AES_128_CBC_SHA256\, TLS_RSA_WITH_AES_256_CBC_SHA\, TLS_RSA_WITH_AES_128_CBC_SHA\, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384\, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256\, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384\, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256\, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA\, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA;
Secure Authentication Sequence Required for Logon	SMB	1
TLSv1.2 Strong Ciphers	SSL	TCP(3389): TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (128-bit)\, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (256-bit)\, TLS_RSA_WITH_AES_128_GCM_SHA256 (128-bit)\, TLS_RSA_WITH_AES_256_GCM_SHA384 (256-bit)
USB Devices Detected on Windows	SMB	Unnamed Devices: ['@usbhub3.inf\,%usbhub3.roothubdevicedesc%;USB Root Hub (USB 3.0)'\, '@usbhub3.inf\,%usbhub3.roothubdevicedesc%;USB Root Hub (USB 3.0)'\, '@usbhub3.inf\,%usbhub3.roothubdevicedesc%;USB Root Hub (USB 3.0)'\, '@usb.inf\,%usb\\\\composite.devicedesc%;USB Composite Device'\, '@usb.inf\,%usb\\\\composite.devicedesc%;USB Composite Device'\, '@usb.inf\,%usb\\\\composite.devicedesc%;USB Composite Device'\, '@input.inf\,%hid.devicedesc%;USB Input Device'\, '@input.inf\,%hid.devicedesc%;USB Input Device'\, '@input.inf\,%hid.devicedesc%;USB Input Device'\, '@input.inf\,%hid.devicedesc%;USB Input Device'\, '@input.inf\,%hid.devicedesc%;USB Input Device'\, '@input.inf\,%hid.devicedesc%;USB Input Device'\, '@usb.inf\,%usb\\\\composite.devicedesc%;USB Composite Device'\, '@usb.inf\,%usb\\\\composite.devicedesc%;USB Composite Device'\, '@usb.inf\,%usb\\\\composite.devicedesc%;USB Composite Device'\, '@input.inf\,%hid.devicedesc%;USB Input Device'\, '@input.inf\,%hid.devicedesc%;USB Input Device'\, '@input.inf\,%hid.devicedesc%;USB Input Device']

continued on next page

Configuration Check	Discovery Method	Value
Unquoted Service Paths	WDRT	BHDrvx64: \??\C:\ProgramData\Symantec\Symantec Endpoint Protection\14.3.8289.5000.105\Data\Definitions\BASHDefs\20240829.001\BHDrvx Symantec Eraser Control driver: \??\C:\Program Files (x86)\Common Files\Symantec Shared\EENGINE\eeCtrl64.sys, EraserUtilRebootDrv: \??\C:\Program Files (x86)\Common Files\Symantec Shared\EENGINE\EraserUtilRebootDrv.sys, IDSvia64: \??\C:\ProgramData\Symantec\Symantec Endpoint Protection\14.3.8289.5000.105\Data\Definitions\IPSDefs\20240830.061\IDSvia64.sys, Symantec Real Time Storage Protection x64: \??\C:\ProgramData\Symantec\Symantec Endpoint Protection\14.3.8289.5000.105\Data\SymPlatform\SRTSP64.SYS, Symantec Eventing Platform: \??\C:\ProgramData\Symantec\Symantec Endpoint Protection\14.3.8289.5000.105\Data\SymPlatform\SymEvnt.sys
WDRT Authentication Success	TCP	True
WDRT Protocol Used	WDRT	SMB Registry and File Access, 64-bit
WDRT_Access	TCP	WDRT_SMB_AUTH_SUCCESS : True, WDRT_SMB_REGISTRY_ACCESS : True, WDRT_SMB_FILE_ACCESS : True, WDRT_RPC_AUTH_SUCCESS : True, WDRT_WMI_AUTH_SUCCESS : True, WDRT_HOST_IS_64BIT : True,
Windows Build Version	WDRT	20348.2655
Windows DRT Access	WDRT	Windows Registry Access: True, CIFS Filesystem Access: True
Windows Edition	WDRT	Windows Server 2022 Standard
Windows IPv6 Setting	WDRT	DisabledComponents registry key is not present. All IPv6 components are enabled.
Windows Installer Version	WDRT	5.0.20348
Windows System Root Directory	SMB	C:\Windows

Vulnerabilities

Vulnerability	CVE	Hosts	Score
MS-2021-Feb: System Center Operations Manager Elevation of Privilege Vulnerability	CVE-2021-1728	1	6
NetBIOS SSN Available		1	0
SMB AUTHENTICATION SUCCESS		1	0
Host has IPv6 Enabled		1	0
RPC DCOM AUTHENTICATION SUCCESS		1	0
WMI AUTHENTICATION SUCCESS		1	0
The contents of an SMB share may be enumerated		1	0
A Windows SMB share permits read access to Everyone [via SMB]		1	0
Microsoft Remote Desktop Service Available		1	0
IP Addresses Enumerated Via NetBIOS		1	0
Portable Storage Devices Detected (Windows)		1	0
BigFix		1	0
No UNC Paths Configured for Integrity		1	0
No UNC Paths Configured for Privacy		1	0
No UNC Paths Configured for Mutual Authentication		1	0
Windows DRT Command Success		1	0
MS15-124: Microsoft Browser ASLR Bypass Vulnerability	CVE-2015-6161	1	0
CredSSP "AllowEncryptionOracle" Policy Setting: Mitigated Mode		1	0
CACHED APPLICATION DATA		1	0
ms-msdt Protocol Scheme Configured		1	0
search-ms Protocol Scheme Configured		1	0
Unquoted Service Path Weakness		1	0
DCE RPC mapper available		1	0
MS-2024-Jul: Windows Cryptographic Services Security Feature Bypass Vulnerability	CVE-2024-30098	1	0

Vulnerability

Vulnerability Name	MS-2021-Feb: System Center Operations Manager Elevation of Privilege Vulnerability	**Score**	6
Published	2021-02-09	**Strategy**	Data-Driven Attack
	nCircle: 475085	**CVSS v2**	6.5
CVSS v3	8.8		

Description

DESCRIPTION
Microsoft System Center 2019 Management Server, Monitoring Agent, and Gateway are subject to an elevation of privilege vulnerability. A local attacker could elevate privileges upon successful exploitation of this vulnerability.
SOLUTION
The vendor has released patches for this vulnerability. Please refer to the advisory links below.

Affected Applications

Application Name
Microsoft System Center Operations Manager 2019
Microsoft System Center Operations Manager Gateway 2019
Microsoft System Center Operations Manager Server 2019
Microsoft System Center Operations Monitoring Agent 2019

Advisory Publisher Entries

CVE:CVE-2021-1728	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1728
CVSSv3 Base Score: 8.8	http://www.tripwire.com/vert/cvss/?data=8.8
CVSSv3 Base Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U	http://www.tripwire.com/vert/cvss/?data=CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I
CWE: 269	http://cwe.mitre.org/data/definitions/269.html
MSRC Guidance: CVE-2021-1728	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1728
Tripwire CVSSv3 Temporal Score: 7.1	http://www.tripwire.com/vert/cvss/?data=7.1
Tripwire CVSSv3 Temporal Vector: (E:U/RL:O/RC:C)	http://www.tripwire.com/vert/cvss/?data=(E:U/RL:O/RC:C)
Tripwire DRT Required: Yes	http://www.tripwire.com/vert/?Yes
Tripwire: Released in ASPL 928 on 2021-02-10	http://www.tripwire.com/vert/?Released in ASPL 928 on 2021-02-10

Rules

```
RegistryQuery GetKey[HKLM\SOFTWARE\Classes\Installer\Patches\28911973A76393B4781D9F71D8DF0060] THEN CHECK NOT
Exists THEN EXECUTE { import smb_file from version import Version as V, VersionException as VE
def get_file_
```

```
version( path, file=r'MOMModules.dll' ):  try:  path = r'%s%s' % (path,file) file_ver = smb_
file.GetFileVersion(rule, None, path) ver = V(None, None, file_ver) except (VE): rule.STOP
(False) return ver
regPath = r'HKLM\SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Setup\InstallDire
ctory' rule.RegistryGetValue(regPath)
if not rule.success:  rule.STOP(False)
path = rule.buffer if get_fi
le_version(path) <= V('10.19.10153.0'):  rule.STOP(True)
rule.STOP(False) }
RegistryQuery GetKey[HKLM\SOFTWARE\Classes\Installer\Patches\361CF1CB9F722F24DBF3262F141DFE75] THEN CHECK NOT
Exists THEN EXECUTE { import smb_file from version import Version as V, VersionException as VE
def get_file_
version( path, file=r'MOMModules.dll' ):  try:  path = r'%s%s' % (path,file) file_ver = smb_
file.GetFileVersion(rule, None, path) ver = V(None, None, file_ver) except (VE): rule.STOP
(False) return ver
regPath = r'HKLM\SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Setup\InstallDire
ctory' rule.RegistryGetValue(regPath)
if not rule.success:  rule.STOP(False)
path = rule.buffer if get_fi
le_version(path) <= V('10.19.10153.0'):  rule.STOP(True)
rule.STOP(False) }
RegistryQuery GetKey[HKLM\SOFTWARE\Classes\Installer\Patches\E1B272A0F1D20974B9842D1CE0355286] THEN CHECK NOT
Exists THEN EXECUTE { import smb_file from version import Version as V, VersionException as VE
def get_file_
version( path, file=r'MOMModules.dll' ):  try:  path = r'%s%s' % (path,file) file_ver = smb_
file.GetFileVersion(rule, None, path) ver = V(None, None, file_ver) except (VE): rule.STOP
(False) return ver
regPath = r'HKLM\SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Setup\InstallDire
ctory' rule.RegistryGetValue(regPath)
if not rule.success:  rule.STOP(False)
path = rule.buffer if get_fi
le_version(path) <= V('10.19.10153.0'):  rule.STOP(True)
rule.STOP(False) }
```

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Vulnerability

Vulnerability Name	NetBIOS SSN Available	**Score**	0
Published	nCircle: 1492	**Strategy**	Access Control Breach
CVSS v3	0.0	**CVSS v2**	0.0

Description

DESCRIPTION
The NetBIOS session service (netBIOS-ssn, tcp 139) serves as a connection-oriented, reliable, sequenced transport mechanism for NetBIOS messages.

The Windows NetBIOS implementation is designed for ease-of-use with regard to network resource sharing. Windows NT/2K allows a substantial amount of information to be obtained about the network by querying NetBIOS services. There are several severe information leaks associated with default configuration of Windows NT: anonymous domain and user enumeration, share access, and remote acquisition of Registry information (a.k.a. the "Red Button" attack).
SOLUTION
We recommend the use of packet filtering on firewalls and border routers to block access to NetBIOS services of internal systems. On systems that are exposed to the Internet, entirely disable the following NetBIOS services over TCP/IP:

NetBIOS Name Service, 137/tcp and 137/udp
NetBIOS Datagram Service, 138/tcp and 138/udp
NetBIOS Session Service, 139/tcp and 139/udp

Affected Applications

Application Name
Microsoft Windows NetBIOS Session Service
NetBIOS Session Service
Samba NBSS

Advisory Publisher Entries

Sans Top 20 2001: W4	http://www.sans.org/top20/2001/?portal=738979f087d735924c39f0d8843ebedf#W4
Sans Top 20 2002: W4	http://www.sans.org/top20/2002/?portal=d545407eee69d45bca553661aa6cd41e#W4
Sans Top 20 2003: w5	http://www.sans.org/top20/2003/?portal=e4f3ca489ec98236af967652e9032da3#w5
Sans Top 20 2004: w3	http://www.sans.org/top20/2004/?portal=a9a59f93888a513a1bfa62e4af857820#w3
Tripwire CVSSv3 Temporal Score: 0.0	http://www.tripwire.com/vert/cvss/?data=0.0
Tripwire CVSSv3 Temporal Vector: (E:U/RL:W/RC:C)	http://www.tripwire.com/vert/cvss/?data=(E:U/RL:W/RC:C)
Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
STOP WITH Match
STOP WITH Match
STOP WITH Match
```

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Vulnerability

Vulnerability Name	SMB AUTHENTICATION SUCCESS	**Score**	0
Published	nCircle: 5923	**Strategy**	Network Reconnaissance
CVSS v3	0.0	**CVSS v2**	0.0

Description

DESCRIPTION
IP360 was able to log into a device, making DRT testing possible on this host.

Affected Applications

Application Name
IPv4 Layer 4
SMB-Auth

Advisory Publisher Entries

Tripwire CVSSv3 Temporal Score: 0.0	http://www.tripwire.com/vert/cvss/?data=0.0
Tripwire CVSSv3 Temporal Vector: (E:U/RL:W/RC:C)	http://www.tripwire.com/vert/cvss/?data=(E:U/RL:W/RC:C)
Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
EXECUTE{ from aspl_env import getHostVariable from aspl_wdrt import ASPL_WDRT
smb_creds = rule.env.target.get
CredentialSet('SMB')
if smb_creds == []:  rule.STOP(False)
try:  host_access = getHostVariable( 'WDRT_
ACCESS' ) except KeyError:  rule.STOP( False )
if not host_access & ASPL_WDRT.WDRT_SMB_AUTH_SUCCESS: r
ule.STOP( False ) }
```

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Vulnerability

Vulnerability Name	Host has IPv6 Enabled	**Score**	0
Published	nCircle: 7875	**Strategy**	Network Reconnaissance
CVSS v3	0.0	**CVSS v2**	0.0

Description

DESCRIPTION
This Windows host is capable of using IPv6 addresses, and this functionality is activated. Although the ability to process IPv6 is not currently a security vulnerability, future developments could lead to increased risk.

Affected Applications

Application Name
Host has IPv6 Enabled
Windows 2003
Windows XP

Advisory Publisher Entries

Tripwire CVSSv3 Temporal Score: 0.0	http://www.tripwire.com/vert/cvss/?data=0.0
Tripwire CVSSv3 Temporal Vector: (E:U/RL:W/RC:C)	http://www.tripwire.com/vert/cvss/?data=(E:U/RL:W/RC:C)
Tripwire DRT Required: Yes	http://www.tripwire.com/vert/?Yes
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
RegistryQuery GetKey[HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6] THEN CHECK Exists
RegistryQuery GetKey[HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6] THEN CHECK Exists
STOP WITH Match
```

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Vulnerability

Vulnerability Name	RPC DCOM AUTHENTICATION SUCCESS	**Score**	0
Published	nCircle: 9971	**Strategy**	Network Reconnaissance
CVSS v3	0.0	**CVSS v2**	0.0

Description

DESCRIPTION
RPC DCOM AUTHENTICATION SUCCESS

Affected Applications

Application Name
IPv4 Layer 4

Advisory Publisher Entries

Tripwire CVSSv3 Temporal Score: 0.0	http://www.tripwire.com/vert/cvss/?data=0.0
Tripwire CVSSv3 Temporal Vector: (E:U/RL:W/RC:C)	http://www.tripwire.com/vert/cvss/?data=(E:U/RL:W/RC:C)
Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
EXECUTE{ from aspl_wmicore import ASPL_WMI from aspl_env import getHostVariable
smb_creds = rule.env.target.g
etCredentialSet('SMB')
if smb_creds == []:  rule.STOP(False)
rule = ASPL_WMI( env ) env.tls[ '__ASPL_rul
e' ] = rule
try:  host_access = getHostVariable( 'WDRT_ACCESS' ) except KeyError:  rule.STOP( False )

if not host_access & rule.WDRT_RPC_AUTH_SUCCESS: rule.STOP( False ) }
```

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Vulnerability

Vulnerability Name	WMI AUTHENTICATION SUCCESS	**Score**	0
Published	nCircle: 9973	**Strategy**	Network Reconnaissance
CVSS v3	0.0	**CVSS v2**	0.0

Description

DESCRIPTION
WMI AUTHENTICATION SUCCESS

Affected Applications

Application Name
IPv4 Layer 4

Advisory Publisher Entries

Tripwire CVSSv3 Temporal Score: 0.0	http://www.tripwire.com/vert/cvss/?data=0.0
Tripwire CVSSv3 Temporal Vector: (E:U/RL:W/RC:C)	http://www.tripwire.com/vert/cvss/?data=(E:U/RL:W/RC:C)
Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
EXECUTE{ from aspl_wdrt import ASPL_WDRT from aspl_env import getHostVariable
smb_creds = rule.env.target.get
CredentialSet('SMB')
if smb_creds == []:  rule.STOP(False)
try:  host_access = getHostVariable( 'WDRT_
ACCESS' ) except KeyError:  rule.STOP( False )
if not host_access & ASPL_WDRT.WDRT_WMI_AUTH_SUCCESS: r
ule.STOP( False ) }
```

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Vulnerability

Vulnerability Name	The contents of an SMB share may be enumerated	**Score**	0
Published	nCircle: 11137	**Strategy**	Network Reconnaissance
CVSS v3	0.0	**CVSS v2**	0.0

Description

DESCRIPTION
The contents of an SMB share may be enumerated, allowing users to view the files in the share.
SOLUTION
The default permissions of a Windows SMB share vary by operating system version. Ensure SMB shares have a secure access control list.

Affected Applications

Application Name
SMB-Auth
Windows Operating System

Advisory Publisher Entries

Tripwire CVSSv3 Temporal Score: 0.0	http://www.tripwire.com/vert/cvss/?data=0.0
Tripwire CVSSv3 Temporal Vector: (E:U/RL:W/RC:C)	http://www.tripwire.com/vert/cvss/?data=(E:U/RL:W/RC:C)
Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
EXECUTE{ import smb_secdes, stdio, HIC from smb_file import FILE
def enumValues( key ):  rule.RegistryEnum
Values( key )
if( rule.success == False ):  return []
temp = rule.buffer.split( "\0" ) te
mp_length = len( temp ) - 1
if( temp_length > -1 and temp[ temp_length ] == "" ):  temp.pop( t
emp_length ) return temp
def enumDir( share ):  dir = FILE( rule, share, '\\' ) rule.CIFSEnumDir(
"%s:%s\\%s" % ( dir.share, dir.path, '*' ) ) if ( rule.success == False ):  return None return
rule.buffer
Shares = enumValues( "HKLM\\System\\CurrentControlSet\\Services\\LanManServer\\Shares" )
matche
d = False
for share in Shares:  if len( share ) == 0:  continue
if not enumDir( share ):
```

```
continue
matched = True HIC.insert_host_data_list( env.target, 'SMB_Shares_Which_Can_Be_Enumer
ated', 'WDRT', share ) continue
if not matched:  rule.STOP( False ) }
EXECUTE{ import smb_secdes, stdio, HIC from smb_file import FILE
try:  if env.getContextVariable( 'SMBAcc
essDenied' ):  rule.STOP( False ) except KeyError:  rule.STOP( False )
def enumShares():  rule.S
MBEnumShares()
if( rule.success == False ):  return []
temp = rule.buffer.split( '\n' ) t
emp_length = len( temp ) - 1
if( temp_length > -1 and temp[ temp_length ] == '' ):  temp.pop( temp
_length ) return temp
def enumDir( share ):  dir = FILE( rule, share, '\\' ) rule.CIFSEnumDir( "%s
:%s\\%s" % ( dir.share, dir.path, '*' ) ) if ( rule.success == False ):  return None return ru
le.buffer
shares = enumShares()
if not shares:  rule.STOP( False )
matched = False
for share in share
s:  if ( len( share ) == 0 ):  continue
if not enumDir( share ):  continue
mat
ched = True HIC.insert_host_data_list( env.target, 'SMB_Shares_Which_Can_Be_Enumerated', 'SMB', share )
continue
if not matched:  rule.STOP( False ) }
```

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Vulnerability

Vulnerability Name	A Windows SMB share permits read access to Everyone [via SMB]	**Score**	0
Published	nCircle: 11144	**Strategy**	Network Reconnaissance
CVSS v3	0.0	**CVSS v2**	0.0

Description

DESCRIPTION
A folder that grants read access to Everyone is accessible through an SMB share.
SOLUTION
The effective permissions of an SMB share are determined by the most restrictive result of the SMB permissions and the underlying file system permissions. Ensure shared folders have a secure access control list.

Affected Applications

Application Name
SMB-Auth

Advisory Publisher Entries

Tripwire CVSSv3 Temporal Score: 0.0	http://www.tripwire.com/vert/cvss/?data=0.0
Tripwire CVSSv3 Temporal Vector: (E:U/RL:W/RC:C)	http://www.tripwire.com/vert/cvss/?data=(E:U/RL:W/RC:C)
Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
EXECUTE{ import smb_secdes, stdio, HIC import smb_file from dp_exceptions import SMBFailure
try:  if env.
getContextVariable( 'SMBAccessDenied' ):  rule.STOP( False ) except KeyError:  rule.STOP( False )
d
ef enumShares():  rule.SMBEnumShares( )
if( rule.success == False ):  return []
temp = rul
e.buffer.split( '\n' ) temp_length = len( temp ) - 1
if( temp_length > -1 and temp[ temp_length ] ==
'' ):  temp.pop( temp_length )
if temp.count( 'IPC$' ):  temp.remove( 'IPC$' )
return
temp
def getDirDacl( share ):  try:  smb_file.GetFileDACL( rule, share, '\\' ) except SMBFailur
e:  rule.success = False
if ( rule.success == False ):  return None return rule.buffer
```

```
shares = enumShares()
matched = False
for share in shares:  if len( share ) == 0:  continue

value = getDirDacl( share )
if not value:  continue
SecDes = smb_secdes.FileObject.UnpackSDD
...
```

Authentication Attempt

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Vulnerability

Vulnerability Name	Microsoft Remote Desktop Service Available	**Score**	0
Published	nCircle: 27350	**Strategy**	Network Reconnaissance
CVSS v3	0.0	**CVSS v2**	0.0

Description

DESCRIPTION
The Microsoft Remote Desktop Service was detected on the server.

The Microsoft Remote Desktop Service (formerly known as Terminal Service) provides remote display and input capabilities over network connections for Windows-based applications running on a server. RDP is designed to support different types of network topologies and multiple LAN protocols. By default the server listens on TCP port 3389.
SOLUTION
Disable this service if it is not essential to the server's operation.

Affected Applications

Application Name
Microsoft Remote Desktop Protocol

Advisory Publisher Entries

Tripwire CVSSv3 Temporal Score: 0.0	http://www.tripwire.com/vert/cvss/?data=0.0
Tripwire CVSSv3 Temporal Vector: (E:U/RL:W/RC:C)	http://www.tripwire.com/vert/cvss/?data=(E:U/RL:W/RC:C)
Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
STOP WITH Match
```

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Vulnerability

Vulnerability Name	IP Addresses Enumerated Via NetBIOS	**Score**	0
Published	nCircle: 28951	**Strategy**	Network Reconnaissance
CVSS v3	0.0	**CVSS v2**	0.0

Description

DESCRIPTION
By sending a NetBIOS query, an attacker may be able to detect all IP Addresses on a system, not just the public IP Address. This may disclose internal network information.
SOLUTION
Restrict access within a broadcast domain to trusted hosts only.

Affected Applications

Application Name
NetBIOS Name Service

Advisory Publisher Entries

Tripwire CVSSv3 Temporal Score: 0.0	http://www.tripwire.com/vert/cvss/?data=0.0
Tripwire CVSSv3 Temporal Vector: (E:U/RL:W/RC:C)	http://www.tripwire.com/vert/cvss/?data=(E:U/RL:W/RC:C)
Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
EXECUTE " import HIC
dataStart = 'zp\x01\x00\x00\x01\x00\x00\x00\x00\x00\x00 ' dataEnd = 'AA\x00\x00 \x00\x01
' new = ''
encodeRef = { 'A' : 'EB', 'B' : 'EC', 'C' : 'ED', 'D' : 'EE', 'E' : 'EF', 'F' : 'EG', 'G'
:  'EH', 'H':'EI', 'I':'EJ','J':'EK', 'K' : 'EL', 'L' : 'EM', 'M' : 'EN', 'N' : 'EO', 'O' : 'EP', 'P' : 'FA
', 'Q' : 'FB', 'R' : 'FC', 'R' : 'FC', 'S' : 'FD', 'T' : 'FE', 'U' : 'FF', 'V' : 'FG', 'W' : 'FH', 'X' : '
FI', 'Y' : 'FJ', 'Z' : 'FK', 'O' :  'DA', '1' :  'DB', '2' :  'DC', '3' :  'DD', '4' :  'DE', '5' :  'DF', '
6' :  'DG', '7' :  'DH', '8' :  'DI', '9' :  'DJ', ' ' :  'CA', '!'  :  'CB', '\x27' :  'CC', '#' :  'CD', '\x24'
:
'CE', '%' :  'CF', '&' :  'CG', '\x27' :  'CH', '(' :  'CI', ')' :  'CJ', '*' :  'CK', '+' :  'CL', ',' :  'C
M', '-' :  'CN', '.'  :  'CO', '=' :  'DN', ':'  :  'DK', ';' :  'DL', '@' :  'EA', '^' :  'FO', '_' :  'FP', '{' :
'HL', '}' :  'HN', '~' :  'HO', }
def encodeName(name):  new = '' for char in name:  new += encod
...
```

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Vulnerability

Vulnerability Name	Portable Storage Devices Detected (Windows)	**Score**	0
Published	nCircle: 47419	**Strategy**	Network Reconnaissance
CVSS v3	0.0	**CVSS v2**	0.0

Description

DESCRIPTION
Portable storage devices are being detected (Windows).

Affected Applications

Application Name
Windows Registry

Advisory Publisher Entries

Tripwire CVSSv3 Temporal Score: 0.0	http://www.tripwire.com/vert/cvss/?data=0.0
Tripwire CVSSv3 Temporal Vector: (E:U/RL:W/RC:C)	http://www.tripwire.com/vert/cvss/?data=(E:U/RL:W/RC:C)
Tripwire DRT Required: Yes	http://www.tripwire.com/vert/?Yes
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
EXECUTE{
from util import enumKeys import HIC
friendlyNameList = [] deviceDescList = [] hasFriendlyNames = F
alse hasDeviceDesc = False
for path1 in enumKeys(rule, "HKLM\\SYSTEM\\CurrentControlSet\\Enum\\USB\\" ):
for path2 in enumKeys( rule, "HKLM\\SYSTEM\\CurrentControlSet\\Enum\\USB\\" + path1 ):  path3 = ("HKLM
\\SYSTEM\\CurrentControlSet\\Enum\\USB\\" + path1 + "\\" + path2) print repr(path3) rule.Regis
tryGetValue(path3 + '\\FriendlyName') if not rule.success:  rule.RegistryGetValue(p
ath3 + '\\DeviceDesc') if rule.success:  deviceDescList.append(rule.buffer) else:
friendlyNameList.append(rule.buffer)
if len(friendlyNameList) > 0:  hasFrie
ndlyNames = True if len(deviceDescList) > 0:  hasDeviceDesc = True
if hasFriendlyNames or hasDeviceDes
c:  if hasFriendlyNames:  friendlyNameString = 'Named Devices:  %s' % str(friendlyNameList) if h
...
```

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Vulnerability

Vulnerability Name	BigFix	**Score**	0
Published	Custom: 100005	**Strategy**	
CVSS v3	0	**CVSS v2**	0

Description

Detect Bigfix

Rules

```
RegistryQuery GetKey[HKLM\SOFTWARE\BigFix\EnterpriseClient] THEN CHECK Exists
RegistryQuery GetKey[HKLM\SOFTWARE\Wow6432Node\BigFix\EnterpriseClient] THEN CHECK Exists
```

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Vulnerability

Vulnerability Name	No UNC Paths Configured for Integrity	**Score**	0
Published	nCircle: 205862	**Strategy**	Data-Driven Attack
CVSS v3	0.0	**CVSS v2**	0.0

Description

DESCRIPTION
There are no hardened UNC paths configured in Group Policy to require the use RequireIntegrity.
SOLUTION
Configure hardened UNC paths in Group Policy to use the RequireIntegry flag as seen in http://support.microsoft.com/kb/3000483.

Affected Applications

Application Name
Windows Domain Joined Host

Advisory Publisher Entries

Tripwire CVSSv3 Temporal Score: 0.0	http://www.tripwire.com/vert/cvss/?data=0.0
Tripwire CVSSv3 Temporal Vector: (E:U/RL:W/RC:C)	http://www.tripwire.com/vert/cvss/?data=(E:U/RL:W/RC:C)
Tripwire DRT Required: Yes	http://www.tripwire.com/vert/?Yes
Tripwire: Released in ASPL 601 on 2015-02-11	http://www.tripwire.com/vert/?Released in ASPL 601 on 2015-02-11

Rules

```
EXECUTE { try:  hardened = env.getHostVariable('hardened_unc_paths') if len(hardened) == 0:  rul
e.STOP(True) except KeyError:  rule.STOP(False)
match = True if hardened:  for unc in hardened:
if hardened[unc]['integrity'] == 1:  match = False
rule.STOP(match) }
```

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Vulnerability

Vulnerability Name	No UNC Paths Configured for Privacy	**Score**	0
Published	nCircle: 205863	**Strategy**	Data-Driven Attack
CVSS v3	0.0	**CVSS v2**	0.0

Description

DESCRIPTION
There are no hardened UNC paths configured in Group Policy to require the use of RequirePrivacy.
SOLUTION
Configure hardened UNC paths in Group Policy to use the RequirePrivacy flag as seen in http://support.microsoft.com/kb/3000483.

Affected Applications

Application Name
Windows Domain Joined Host

Advisory Publisher Entries

Tripwire CVSSv3 Temporal Score: 0.0	http://www.tripwire.com/vert/cvss/?data=0.0
Tripwire CVSSv3 Temporal Vector: (E:U/RL:W/RC:C)	http://www.tripwire.com/vert/cvss/?data=(E:U/RL:W/RC:C)
Tripwire DRT Required: Yes	http://www.tripwire.com/vert/?Yes
Tripwire: Released in ASPL 601 on 2015-02-11	http://www.tripwire.com/vert/?Released in ASPL 601 on 2015-02-11

Rules

```
EXECUTE { try:  hardened = env.getHostVariable('hardened_unc_paths') if len(hardened) == 0:  rul
e.STOP(True) except KeyError:  rule.STOP(False)
match = True if hardened:  for unc in hardened:
if hardened[unc]['privacy'] == 1:  match = False
rule.STOP(match) }
```

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Vulnerability

Vulnerability Name	No UNC Paths Configured for Mutual Authentication	**Score**	0
Published	nCircle: 205864	**Strategy**	Data-Driven Attack
CVSS v3	0.0	**CVSS v2**	0.0

Description

DESCRIPTION
There are no hardened UNC paths configured in Group Policy to require the use of Mutual Authentication.
SOLUTION
Configure hardened UNC paths in Group Policy to use the RequireAuthentication flag as seen in http://support.microsoft.com/kb/3000483.

Affected Applications

Application Name
Windows Domain Joined Host

Advisory Publisher Entries

Tripwire CVSSv3 Temporal Score: 0.0	http://www.tripwire.com/vert/cvss/?data=0.0
Tripwire CVSSv3 Temporal Vector: (E:U/RL:W/RC:C)	http://www.tripwire.com/vert/cvss/?data=(E:U/RL:W/RC:C)
Tripwire DRT Required: Yes	http://www.tripwire.com/vert/?Yes
Tripwire: Released in ASPL 601 on 2015-02-11	http://www.tripwire.com/vert/?Released in ASPL 601 on 2015-02-11

Rules

```
EXECUTE { try:  hardened = env.getHostVariable('hardened_unc_paths') if len(hardened) == 0:  rul
e.STOP(True) except KeyError:  rule.STOP(False)
match = True if hardened:  for unc in hardened:
if hardened[unc]['authentication'] == 1:  match = False
rule.STOP(match) }
```

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Vulnerability

Vulnerability Name	Windows DRT Command Success	**Score**	0
Published	nCircle: 211953	**Strategy**	Network Reconnaissance
CVSS v3	0.0	**CVSS v2**	0.0

Description

DESCRIPTION
IP360 was able to successfully access the registry and/or file system using the provided credentials.

Affected Applications

Application Name
Windows Registry

Advisory Publisher Entries

Tripwire CVSSv3 Temporal Score: 0.0	http://www.tripwire.com/vert/cvss/?data=0.0
Tripwire CVSSv3 Temporal Vector: (E:U/RL:U/RC:C)	http://www.tripwire.com/vert/cvss/?data=(E:U/RL:U/RC:C)
Tripwire DRT Required: Yes	http://www.tripwire.com/vert/?Yes
Tripwire: Released in ASPL 615 on 2015-05-16	http://www.tripwire.com/vert/?Released in ASPL 615 on 2015-05-16

Rules

```
EXECUTE{ import smb_file, HIC registry_access = False cifs_system_access = False rule.RegistryGetValue(r'HKLM\
Software\Microsoft\Windows NT\CurrentVersion\SystemRoot')
data = 'Windows Registry Access:  %s, CIFS Filesyste
m Access:  %s'
if rule.success:  registry_access = True smb_file.CheckPathExists(rule, '', rule.buf
fer) if rule.success:  cifs_system_access = True
data = data % ( str( registry_access ), str( cifs
_system_access ) ) HIC.insert_host_data(env.target, 'windows_drt_access', 'WDRT', data) if cifs_system_access
and registry_access:  rule.STOP( True ) rule.STOP( False ) }
```

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Vulnerability

Vulnerability Name	MS15-124: Microsoft Browser ASLR Bypass Vulnerability	**Score**	0
Published	nCircle: 220130	**Strategy**	Network Reconnaissance
CVSS v3	0.0	**CVSS v2**	4.3

Description

DESCRIPTION
Microsoft Browser contains an ASLR Bypass Vulnerability. The vulnerability could allow an attacker to bypass the Address Space Layout Randomization (ASLR) security feature.
SOLUTION
The vendor has released patches for this vulnerability. Please refer to the advisory links below.

Affected Applications

Application Name
Microsoft Internet Explorer 10
Microsoft Internet Explorer 11
Microsoft Internet Explorer 7
Microsoft Internet Explorer 8
Microsoft Internet Explorer 9
Windows Registry

Advisory Publisher Entries

BugTraq: 78537	http://www.securityfocus.com/bid/78537
CVE:CVE-2015-6161	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6161
CWE: 200	http://cwe.mitre.org/data/definitions/200.html
MS Advisory Number: MS15-124	http://technet.microsoft.com/en-us/security/bulletin/MS15-124
MS Hotfix Number: 3104002	http://support.microsoft.com/default.aspx?scid=KB;en-us;3104002
Tripwire CVSSv3 Temporal Score: 0.0	http://www.tripwire.com/vert/cvss/?data=0.0
Tripwire CVSSv3 Temporal Vector: (E:U/RL:O/RC:C)	http://www.tripwire.com/vert/cvss/?data=(E:U/RL:O/RC:C)
Tripwire DRT Required: Yes	http://www.tripwire.com/vert/?Yes
Tripwire: Released in ASPL 648 on 2015-12-09	http://www.tripwire.com/vert/?Released in ASPL 648 on 2015-12-09

Rules

```
EXECUTE { from smbutil import getKnownFileVersionObj from version import Version as V, VersionException import
smb_file import aspl_env
def get_file_version(system_root, file = 'win32k.sys'):  try:  path = '%s
\\system32\\%s' % (system_root,file) file_ver = smb_file.GetFileVersion(rule, None, path) ver
= V(None, None, file_ver) except VersionException:  rule.STOP(False) return ver
try:
```

```
win_ver = aspl_env.getHostVariable('windows_version') system_root = env.getHostVariable('windows_system
_root_directory') except KeyError:  rule.STOP( False )
try:  is64 = env.getContextVariable('host_is_64_
bit') except KeyError:  is64 = False
keys = [r'HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureContr
ol\FEATURE_ALLOW_USER32_EXCEPTION_HANDLER_HARDENING\iexplore.exe'] if is64:  keys.append(r'HKLM\SOFTWARE\Wo
w6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ALLOW_USER32_EXCEPTION_HANDLER_HARDENING\iex
...
EXECUTE { from smbutil import getKnownFileVersionObj from version import Version as V, VersionException import
smb_file import aspl_env
def get_file_version(system_root, file = 'win32k.sys'):  try:  path = '%s
\\system32\\%s' % (system_root,file) file_ver = smb_file.GetFileVersion(rule, None, path) ver
= V(None, None, file_ver) except VersionException:  rule.STOP(False) return ver
try:
win_ver = aspl_env.getHostVariable('windows_version') system_root = env.getHostVariable('windows_system
_root_directory') except KeyError:  rule.STOP( False )
try:  is64 = env.getContextVariable('host_is_64_
bit') except KeyError:  is64 = False
keys = [r'HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureContr
ol\FEATURE_ALLOW_USER32_EXCEPTION_HANDLER_HARDENING\iexplore.exe'] if is64:  keys.append(r'HKLM\SOFTWARE\Wo
w6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ALLOW_USER32_EXCEPTION_HANDLER_HARDENING\iex
...
EXECUTE { from smbutil import getKnownFileVersionObj from version import Version as V, VersionException import
smb_file import aspl_env
def get_file_version(system_root, file = 'win32k.sys'):  try:  path = '%s
\\system32\\%s' % (system_root,file) file_ver = smb_file.GetFileVersion(rule, None, path) ver
= V(None, None, file_ver) except VersionException:  rule.STOP(False) return ver
try:
win_ver = aspl_env.getHostVariable('windows_version') system_root = env.getHostVariable('windows_system
_root_directory') except KeyError:  rule.STOP( False )
try:  is64 = env.getContextVariable('host_is_64_
bit') except KeyError:  is64 = False
keys = [r'HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureContr
ol\FEATURE_ALLOW_USER32_EXCEPTION_HANDLER_HARDENING\iexplore.exe'] if is64:  keys.append(r'HKLM\SOFTWARE\Wo
w6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ALLOW_USER32_EXCEPTION_HANDLER_HARDENING\iex
...
EXECUTE { from smbutil import getKnownFileVersionObj from version import Version as V, VersionException import
smb_file import aspl_env
def get_file_version(system_root, file = 'win32k.sys'):  try:  path = '%s
\\system32\\%s' % (system_root,file) file_ver = smb_file.GetFileVersion(rule, None, path) ver
= V(None, None, file_ver) except VersionException:  rule.STOP(False) return ver
try:
win_ver = aspl_env.getHostVariable('windows_version') system_root = env.getHostVariable('windows_system
_root_directory') except KeyError:  rule.STOP( False )
try:  is64 = env.getContextVariable('host_is_64_
bit') except KeyError:  is64 = False
keys = [r'HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureContr
ol\FEATURE_ALLOW_USER32_EXCEPTION_HANDLER_HARDENING\iexplore.exe'] if is64:  keys.append(r'HKLM\SOFTWARE\Wo
w6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ALLOW_USER32_EXCEPTION_HANDLER_HARDENING\iex
```

...

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Vulnerability

Vulnerability Name	CredSSP "AllowEncryptionOracle" Policy Setting: Mitigated Mode	**Score**	0
Published	nCircle: 385173	**Strategy**	Network Reconnaissance
CVSS v3	0.0	**CVSS v2**	0.0

Description

DESCRIPTION
The system has the AllowEncryptionOracle policy set to Mitigated mode. Client applications that use CredSSP will not be able to fall back to insecure versions, but services that use CredSSP will accept unpatched clients.
SOLUTION
This exposure is for informational purposes only. For more information about the AllowEncryptionOracle policy modes refer to Microsoft's KB4093492.

Affected Applications

Application Name
Windows Registry

Advisory Publisher Entries

MS Hotfix Number: 4093492	http://support.microsoft.com/default.aspx?scid=KB;en-us;4093492
Tripwire CVSSv3 Temporal Score: 0.0	http://www.tripwire.com/vert/cvss/?data=0.0
Tripwire CVSSv3 Temporal Vector: (E:U/RL:W/RC:C)	http://www.tripwire.com/vert/cvss/?data=(E:U/RL:W/RC:C)
Tripwire DRT Required: Yes	http://www.tripwire.com/vert/?Yes
Tripwire: Released in ASPL 783 on 2018-06-19	http://www.tripwire.com/vert/?Released in ASPL 783 on 2018-06-19

Rules

```
EXECUTE { import smb_file from version import Version as V, VersionException as VE from HIC import insert_host
_data_list
hicName = "allow_encryption_oracle" vulnerable = False default_policy = False
rule.RegistryGetVal
ue( r'HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\CredSSP\Parameters\AllowEncryptionOracle'
) if not rule.success:  mode = "AllowEncryptionOracle is not set." default_policy = True elif rule.buff
er=="0x00000002":  mode = "AllowEncryptionOracle registry reports vulnerable mode (%s)." % rule.buffer
vulnerable = True elif rule.buffer=="0x00000001":  mode = "AllowEncryptionOracle registry reports client mi
tigation mode (%s)." % rule.buffer elif rule.buffer=="0x00000000":  mode = "AllowEncryptionOracle registry
reports force updated clients mode (%s)." % rule.buffer insert_host_data_list( env.target, hicName, 'WDRT'
, mode) rule.STOP(False)
try:  win_ver = env.getHostVariable( 'windows_version' ) except KeyError:
```

...

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Vulnerability

Vulnerability Name	CACHED APPLICATION DATA	**Score**	0
Published	nCircle: 479266	**Strategy**	Network Reconnaissance
CVSS v3	0.0	**CVSS v2**	0.0

Description

DESCRIPTION
The instance data of this vulnerability contains the data stored in the cache after the application scan.

Affected Applications

Application Name
Windows Registry

Advisory Publisher Entries

Tripwire CVSSv3 Temporal Score: 0.0	http://www.tripwire.com/vert/cvss/?data=0.0
Tripwire CVSSv3 Temporal Vector: (E:U/RL:U/RC:C)	http://www.tripwire.com/vert/cvss/?data=(E:U/RL:U/RC:C)
Tripwire DRT Required: Yes	http://www.tripwire.com/vert/?Yes
Tripwire: Released in ASPL 937 on 2021-03-30	http://www.tripwire.com/vert/?Released in ASPL 937 on 2021-03-30

Rules

```
EXECUTE { try:  data = env.getContextVariable('ASPLCache')[0] pretty_data = '' try:  for que
ry, item in data:  pretty_data += '%s %s\n' % (query, item) pretty_data += '\t%s\n' % s
tr(data[(query, item)]) except MemoryError:  pass rule.transcript = pretty_data rule.transc
riptIsFull = True except KeyError:  pass }
```

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Vulnerability

Vulnerability Name	ms-msdt Protocol Scheme Configured	**Score**	0
Published	nCircle: 529971	**Strategy**	Data-Driven Attack
CVSS v3	0.0	**CVSS v2**	0.0

Description

DESCRIPTION
The ms-msdt protocol scheme is configured on this system. This protocol scheme has been associated with the Follina vulnerability allowing for remote code execution within Microsoft Office.
SOLUTION
Protocol Schemes can be deleted from the registry (HKCR) to remove the association.

Affected Applications

Application Name
Windows Registry

Advisory Publisher Entries

Tripwire CVSSv3 Temporal Score: 0.0	http://www.tripwire.com/vert/cvss/?data=0.0
Tripwire CVSSv3 Temporal Vector: (E:U/RL:W/RC:C)	http://www.tripwire.com/vert/cvss/?data=(E:U/RL:W/RC:C)
Tripwire DRT Required: Yes	http://www.tripwire.com/vert/?Yes
Tripwire: Released in ASPL 1005 on 2022-05-31	http://www.tripwire.com/vert/?Released in ASPL 1005 on 2022-05-31

Rules

```
RegistryQuery GetKey[HKCR\ms-msdt] THEN CHECK Exists
```

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Vulnerability

Vulnerability Name	search-ms Protocol Scheme Configured	**Score**	0
Published	nCircle: 530236	**Strategy**	Data-Driven Attack
CVSS v3	0.0	**CVSS v2**	0.0

Description

DESCRIPTION
The search-ms protocol scheme is configured on this system. This protocol scheme can allow an attacker to open an Explorer window which points at a remote share with a custom display name, potentially allowing the end user to be social engineered.
SOLUTION
Protocol Schemes can be deleted from the registry (HKCR) to remove the association.

Affected Applications

Application Name
Windows Registry

Advisory Publisher Entries

Tripwire CVSSv3 Temporal Score: 0.0	http://www.tripwire.com/vert/cvss/?data=0.0
Tripwire CVSSv3 Temporal Vector: (E:U/RL:W/RC:C)	http://www.tripwire.com/vert/cvss/?data=(E:U/RL:W/RC:C)
Tripwire DRT Required: Yes	http://www.tripwire.com/vert/?Yes
Tripwire: Released in ASPL 1006 on 2022-06-04	http://www.tripwire.com/vert/?Released in ASPL 1006 on 2022-06-04

Rules

```
RegistryQuery GetKey[HKCR\search-ms] THEN CHECK Exists
```

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Vulnerability

Vulnerability Name	Unquoted Service Path Weakness	**Score**	0
Published	nCircle: 530548	**Strategy**	Data-Driven Attack
CVSS v3	0.0	**CVSS v2**	0.0

Description

DESCRIPTION
A vulnerability exists due to the way in which the CreateProcess function creates new processes. When a process path contains spaces, the CreateProcess function attempts to execute a process at each point where a spaces occurs. For example, in the path C:\Program Files\Tripwire Demo\example.exe, the CreateProcess function will attempt to execute C:\Program.exe and C:\Program Files\Tripwire.exe before trying C:\Program Files\Tripwire Demo\example.exe.

This vulnerability can be exploited when services do not properly enclose paths with spaces within quotes.
SOLUTION
Ensure that all executable service paths are wrapped in quotes.

Affected Applications

Application Name
Windows Registry

Advisory Publisher Entries

CWE: 428	http://cwe.mitre.org/data/definitions/428.html
Tripwire CVSSv3 Temporal Score: 0.0	http://www.tripwire.com/vert/cvss/?data=0.0
Tripwire CVSSv3 Temporal Vector: (E:U/RL:W/RC:C)	http://www.tripwire.com/vert/cvss/?data=(E:U/RL:W/RC:C)
Tripwire DRT Required: Yes	http://www.tripwire.com/vert/?Yes
Tripwire: Released in ASPL 1007 on 2022-06-15	http://www.tripwire.com/vert/?Released in ASPL 1007 on 2022-06-15

Rules

```
EXECUTE { import HIC import aspl_env
reg_path = 'HKLM\\System\\CurrentControlSet\\Services' try:  system_root
= aspl_env.getHostVariable('windows_system_root_directory').lower() except KeyError:  rule.STOP(False) unquote
d_paths = [] services = [] system_paths = [ '%systemroot%\\system32\\svchost.exe ', '%systemroot%\\sys
tem32\\dllhost.exe ', '%systemroot%\\system32\\msiexec.exe ', ]
def test_unquoted_path(path, modified
_path):  if ' ' not in path:  return False elif filter_system_paths(path):  return False
elif path.startswith('"') and path.endswith('"'):  return False elif path.startswith("'") and p
ath.endswith("'"):  return False elif split_and_test(path, "'"):  return False elif spl
it_and_test(path, '"'):  return False elif find_valid_spaces(modified_path):  return False
return True
def filter_system_paths(path):  for system_path in system_paths:  if path.startswith
```

...

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Vulnerability

Vulnerability Name	DCE RPC mapper available	**Score**	0
Published	nCircle: 1225	**Strategy**	Network Reconnaissance
CVSS v3	0.0	**CVSS v2**	0.0

Description

DESCRIPTION
DCE is Microsoft's implementation of the RPC protocol.

Microsoft uses DCE in the same manner that Unix uses portmap. This service is used to register other services with a central control program that facilitates distributed computing.

This service can be used by an attacker to determine the name, version, and location of any DCOM or RPC service on the machine.

Affected Applications

Application Name
DCE/MS RPC over TCP

Advisory Publisher Entries

Tripwire CVSSv3 Temporal Score: 0.0	http://www.tripwire.com/vert/cvss/?data=0.0
Tripwire CVSSv3 Temporal Vector: (E:U/RL:W/RC:C)	http://www.tripwire.com/vert/cvss/?data=(E:U/RL:W/RC:C)
Tripwire DRT Required: No	http://www.tripwire.com/vert/?No
Tripwire: N/A	http://www.tripwire.com/vert/?N/A

Rules

```
STOP WITH Match
```

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Vulnerability

Vulnerability Name	MS-2024-Jul: Windows Cryptographic Services Security Feature Bypass Vulnerability	**Score**	0
Published	2024-07-09	**Strategy**	Data-Driven Attack
	nCircle: 644468	**CVSS v2**	2.4
CVSS v3	7.5		

Description

DESCRIPTION
Windows Cryptographic Services are subject to a security feature bypass vulnerability. A local attacker could bypass digital signatures upon successful exploitation of this vulnerability. Successful exploitation requires the attacker to create a SHA1 has collision.
SOLUTION
The vendor has released patches for this vulnerability. Please refer to the advisory links below.

The patch alone does not resolve this vulnerability. The registry key HKLM\SOFTWARE\Microsoft\Cryptography\Calais\DisableCapiOverrideForRSA must also be set to 1.

Affected Applications

Application Name
Microsoft Cryptographic Services

Advisory Publisher Entries

CVE:CVE-2024-30098	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-30098
CVSSv3 Base Score: 7.5	http://www.tripwire.com/vert/cvss/?data=7.5
CVSSv3 Base Vector: CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U	http://www.tripwire.com/vert/cvss/?data=CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I
CWE: 327	http://cwe.mitre.org/data/definitions/327.html
MSRC Guidance: CVE-2024-30098	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-30098
Tripwire CVSSv3 Temporal Score: 3.9	http://www.tripwire.com/vert/cvss/?data=3.9
Tripwire CVSSv3 Temporal Vector: (E:U/RL:O/RC:C)	http://www.tripwire.com/vert/cvss/?data=(E:U/RL:O/RC:C)
Tripwire DRT Required: Yes	http://www.tripwire.com/vert/?Yes
Tripwire: Released in ASPL 1114 on 2024-07-10	http://www.tripwire.com/vert/?Released in ASPL 1114 on 2024-07-10

Rules

```
EXECUTE { import smb_file from version import Version as V, VersionException as VE from util import hexToInt
```

```
def getRegKeyValue(default_value=0):  rule.RegistryGetValue(r'HKLM\SOFTWARE\Microsoft\Cryptography\Calais\D
isableCapiOverrideForRSA') if rule.success:  return hexToInt(rule.buffer) else:  return
default_value
try:  win_ver = env.getHostVariable( 'windows_version' ) except KeyError:  rule.STOP( Fal
se )
def get_file_version( path, file=r'system32\ntoskrnl.exe' ):  try:  path = r'%s\\%s' % (path,f
ile) file_ver = smb_file.GetFileVersion(rule, None, path) ver = V(None, None, file_ver) ex
cept (VE): rule.STOP(False) return ver
try:  path = env.getHostVariable('windows_system_root_d
irectory') except KeyError:  rule.STOP(False)
# Vulnerable before July 2024 Patch if win_ver.startswith( '
10.0.0.0' ) and V( '10.0' ) <= get_file_version( path ) < V( '10.0.10240.20708' ):  rule.STOP(True) elif wi
...
```

Hosts

Hostname	IP Address	Score
WB5VSNATMD001.myl.com	10.250.132.106	6

Applications

Service	Application	Hosts
DCE/MS RPC over TCP	DCE/MS RPC Endpoint Mapper Interface (TCP)	1
Direct SMB Hosting Service	Microsoft Windows OS Family 21H2 Direct SMB Session Service	1
IPv4 Layer 4		1
Microsoft Remote Desktop Protocol		1
Multi-Port Protocol	AllJoyn Router Service	1
Multi-Port Protocol	CNG Key Isolation Service	1
Multi-Port Protocol	DirectWrite	1
Multi-Port Protocol	DirectX 10.x	1
Multi-Port Protocol	DirectX 11.x	1
Multi-Port Protocol	DirectX 12.x	1
Multi-Port Protocol	DirectX 9.0c	1
Multi-Port Protocol	HCL BigFix Client 10.0.7.52	1
Multi-Port Protocol	Host has IPv6 Enabled	1
Multi-Port Protocol	HTTP Service	1
Multi-Port Protocol	IKE and AuthIP IPsec Keying Modules Service	1
Multi-Port Protocol	Ink Support Feature	1
Multi-Port Protocol	IPSec Policy Agent Service	1
Multi-Port Protocol	Microsoft .NET Framework v4.8.x	1
Multi-Port Protocol	Microsoft Cryptographic Services	1
Multi-Port Protocol	Microsoft Internet Explorer 11	1
Multi-Port Protocol	Microsoft JET Database Engine	1
Multi-Port Protocol	Microsoft JScript	1
Multi-Port Protocol	Microsoft Korean Language IME	1
Multi-Port Protocol	Microsoft MDAC	1
Multi-Port Protocol	Microsoft Paint	1
Multi-Port Protocol	Microsoft Remote Desktop Protocol 10.0	1
Multi-Port Protocol	Microsoft SharePoint	1
Multi-Port Protocol	Microsoft SoftGrid/Application Virtualization	1
Multi-Port Protocol	Microsoft System Center Operations Monitoring Agent 2019	1
Multi-Port Protocol	Microsoft Terminal Services Client	1
Multi-Port Protocol	Microsoft VBScript	1
Multi-Port Protocol	Microsoft Visual Studio	1
Multi-Port Protocol	Microsoft Windows Server	1
Multi-Port Protocol	Microsoft Windows Telnet Client	1
Multi-Port Protocol	Mozilla Application	1
Multi-Port Protocol	MPEG Layer-3 codecs	1
Multi-Port Protocol	MSXML 3.0	1
Multi-Port Protocol	MSXML 6.0	1
Multi-Port Protocol	Print Spooler Service	1
Multi-Port Protocol	Remote Registry Service	1
Multi-Port Protocol	Smart Card Service	1
Multi-Port Protocol	SSDP Discovery Service (UPNP)	1
Multi-Port Protocol	Symantec AntiVirus	1
Multi-Port Protocol	Symantec Endpoint Protection Client	1
Multi-Port Protocol	Telephony Service	1

continued on next page

Service	Application	Hosts
Multi-Port Protocol	USB Attached SCSI Protocol Service	1
Multi-Port Protocol	VMware Tools 12.x	1
Multi-Port Protocol	Volume Shadow Copy Service	1
Multi-Port Protocol	Windows Address Book	1
Multi-Port Protocol	Windows ATL Component	1
Multi-Port Protocol	Windows CloudExperienceHost Broker	1
Multi-Port Protocol	Windows Domain Joined Host	1
Multi-Port Protocol	Windows Mail	1
Multi-Port Protocol	Windows Media Player 12	1
Multi-Port Protocol	Windows OpenSSH Client	1
Multi-Port Protocol	Windows OS (Not Server Core)	1
Multi-Port Protocol	Windows Projected File System	1
Multi-Port Protocol	Windows Remote Access Connection Manager	1
Multi-Port Protocol	Windows Remote Desktop Available	1
Multi-Port Protocol	Windows Script Host	1
Multi-Port Protocol	Windows Search / Windows Desktop Search	1
Multi-Port Protocol	Windows Secure Boot Enabled	1
Multi-Port Protocol	Windows Server 2022	1
Multi-Port Protocol	Windows Workstation Service	1
Multi-Port Protocol	WordPad	1
NetBIOS Name Service	Windows NetBIOS Name Service	1
NetBIOS Session Service	Microsoft Windows OS Family 21H2 NetBIOS Session Service	1
Open TCP Port	N/A	1
SMB-Auth	N/A	1
SMB-Registry	N/A	1

Audits

Network Name	Scan Profile Name	Audit Start	Audit End	Approx Hours Taken
A_AHS_Scan2_NoSIH	_Mylan: Standard Profile	09/03/2024 08:10	09/03/2024 08:17	00:06