TECHNICAL ANALYSIS

Fri September 13, 2024

Networks

A_AHS_Scan4_NoSIH

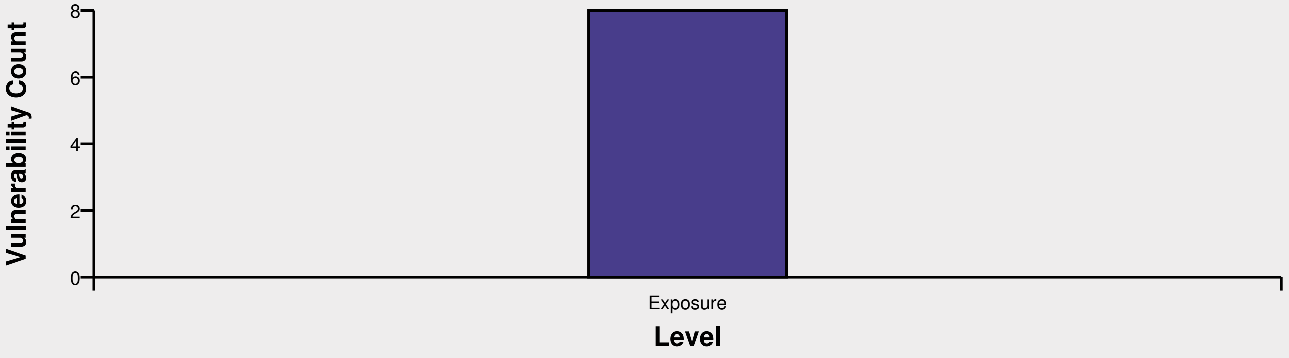
Filters

Windows OS Only

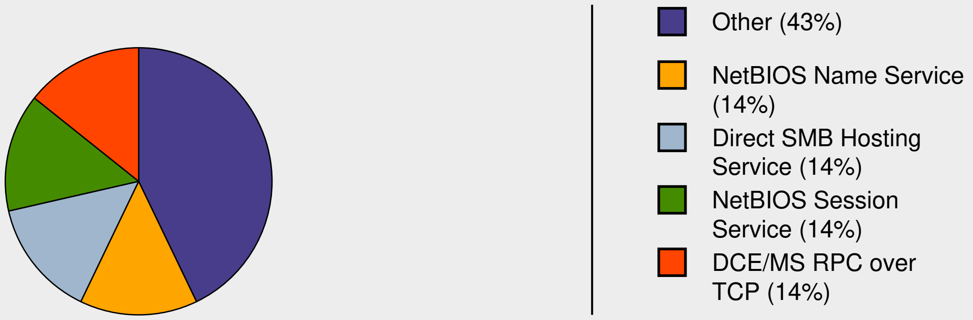
Report Summary

Networks/Network Groups	A_AHS_Scan4_NoSIH	**Filters**	Windows OS Only
Hosts	1	**Asset Value**	0
Average Host Score	0	**Vulnerabilities**	8
Applications/Services	8		

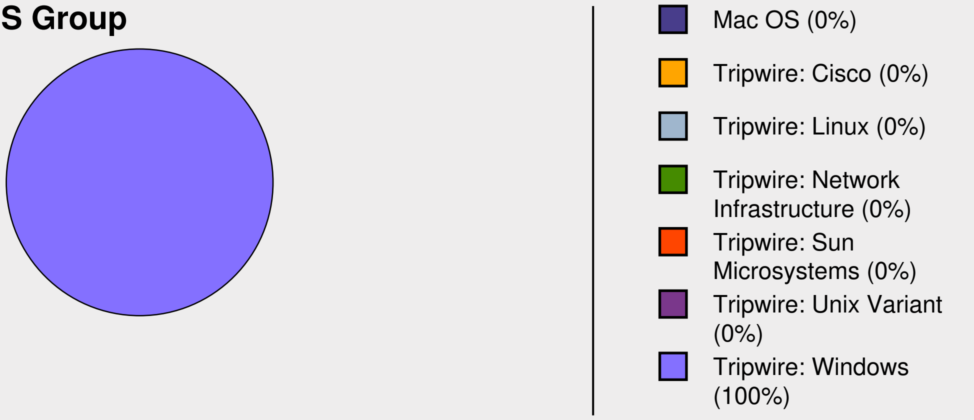
Vulnerability Level Distribution



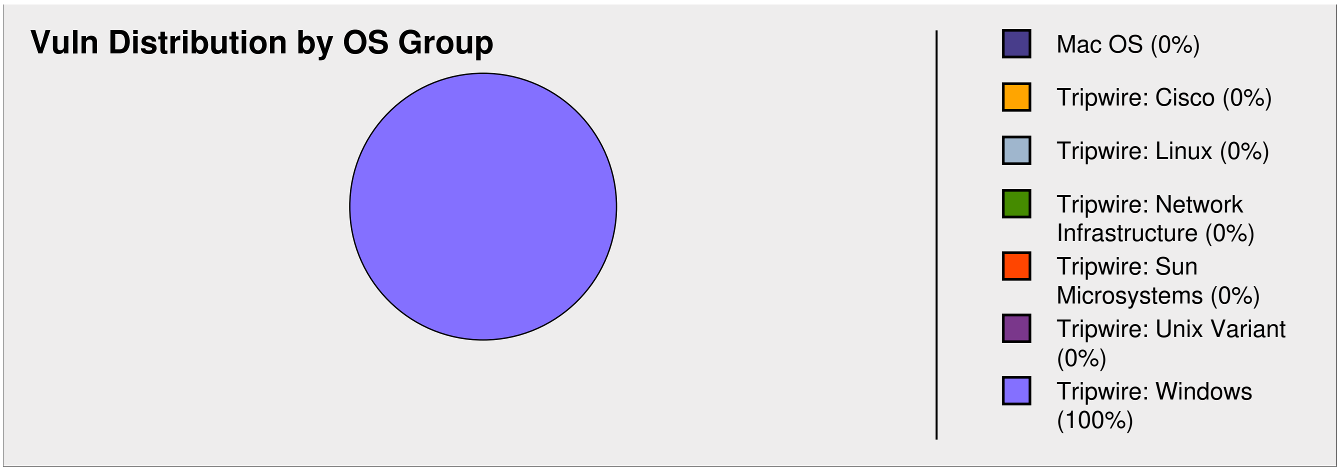
Service Distribution



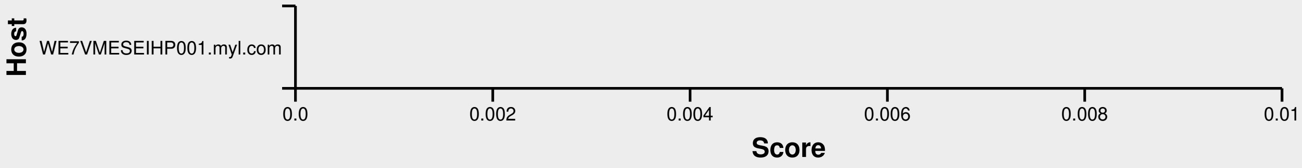
OS Distribution by OS Group



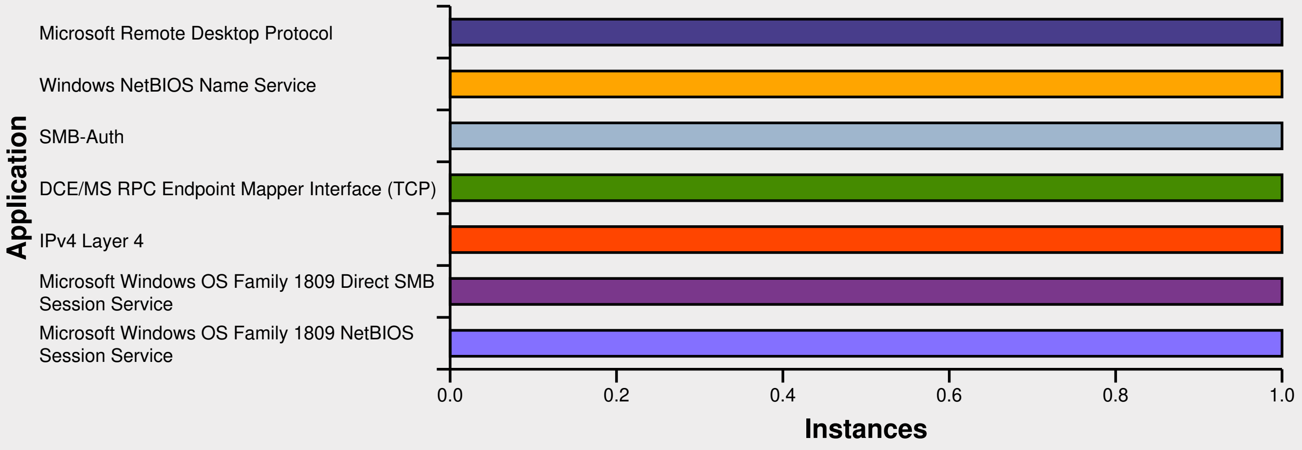
Vuln Distribution by OS Group



Top 10 Most Vulnerable Hosts



Top 10 Applications by Instance



Hosts

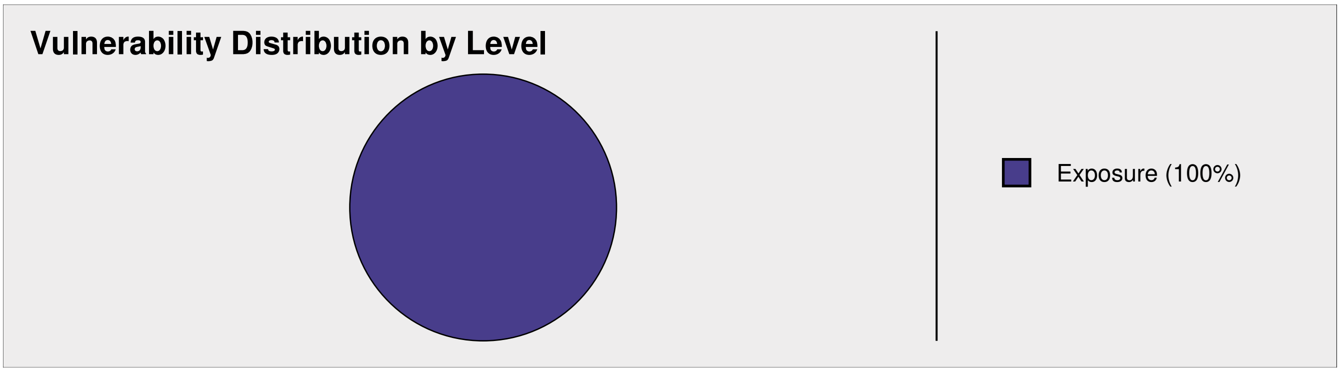
Hostname	IP Address	OS	Agent	Owner	Asset Value	Score
WE7VMESEIHP0	10.4.37.106	Windows 10 OS Family 1809	No	None	0	0

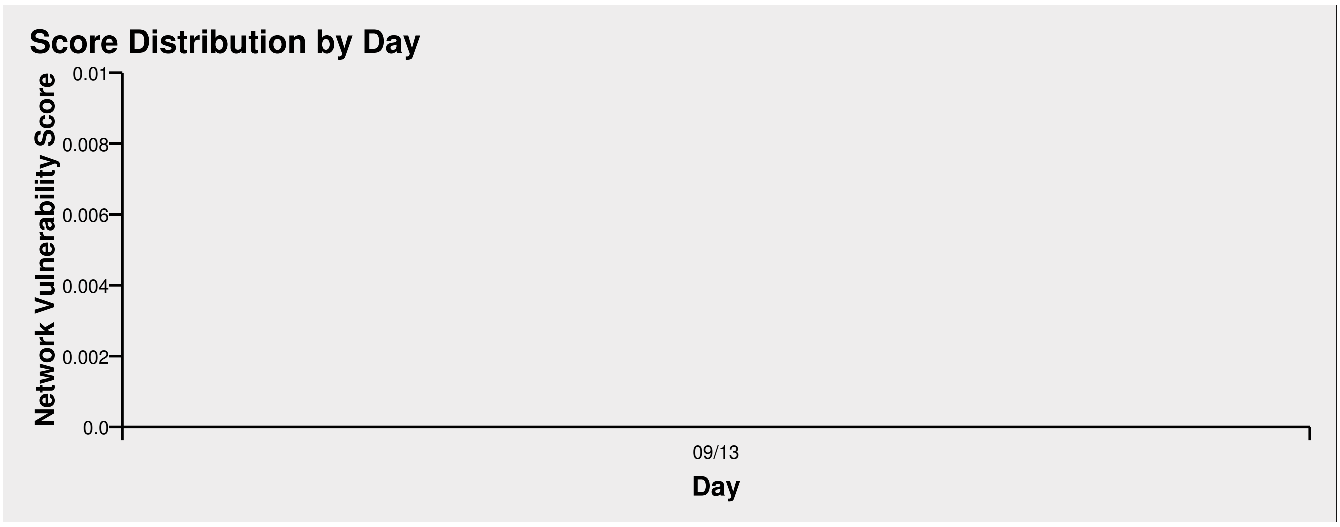
Host Summary

Hostname	WE7VMESEIHP001.myl.com	**IP Address**	10.4.37.106
Score	0	**Asset Value**	0
OS Name	Windows 10 OS Family 1809	**Owner**	None
NetBIOS Name	WE7VMESEIHP001	**Mac Address (NetBIOS)**	
Domain/Workgroup	MYL		

Operating System

OS Name
Windows 10 OS Family 1809





Vulnerabilities

Vulnerability	**CVE**	**# of Ports**	**Score**
DCE RPC mapper available		1	0

continued on next page

Vulnerability	CVE	# of Ports	Score
NetBIOS SSN Available		1	0
SMB AUTHENTICATION FAILURE		1	0
RPC DCOM AUTHENTICATION FAILURE		1	0
WMI AUTHENTICATION FAILURE		1	0
Microsoft Remote Desktop Service Available		1	0
IP Addresses Enumerated Via NetBIOS		1	0
SSL Server Supports CBC Ciphers for TLSv1 Encrypted RDP Sessions		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 1809 Direct SMB Session Service	445
IPv4 Layer 4		0
Microsoft Remote Desktop Protocol		3389
NetBIOS Name Service	Windows NetBIOS Name Service	137
NetBIOS Session Service	Microsoft Windows OS Family 1809 NetBIOS Session Service	139
Open TCP Port	N/A	1556
Open TCP Port	N/A	443
SMB-Auth	N/A	0

Configuration Checks

Configuration Check	Discovery Method	Value
DNS Computer Name	TCP	TCP(139): WE7VMESEIHP001.myl.com, TCP(445): WE7VMESEIHP001.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	10.4.37.106
Netbios Computer Name	TCP	TCP(139): WE7VMESEIHP001, TCP(445): WE7VMESEIHP001
Netbios Domain Name	TCP	TCP(139): MYL, TCP(445): MYL
Nmap OS String	TCP	
Nmap Status	NMAP	Global: Nmap Not Configured
SSL Certificate Extended Key Usage	SSL	TCP(3389): serverAuth
SSL Certificate Issuer	SSL	TCP(3389): commonName=WE7VMESEIHP001.myl.com
SSL Certificate Key Usage	SSL	TCP(3389): keyEncipherment dataEncipherment
SSL Certificate MD5 Thumbprint	SSL	TCP(3389): 39:A1:D8:73:96:F9:0F:68:56:58:7B:EB:C7:BF:3F:2C
SSL Certificate Public Key Size	SSL	TCP(3389): 2048 bits
SSL Certificate SHA1 Thumbprint	SSL	TCP(3389): 5E:2C:18:8B:96:E6:02:82:3C:EA:DD:1F:5C:70:02:28:F7:FB:AA:5A
SSL Certificate Serial Number	SSL	TCP(3389): 17:8C:BD:5F:16:95:AD:A6:46:C6:A5:5B:A5:A8:6C:65

continued on next page

Configuration Check	Discovery Method	Value
SSL Certificate Signature Algorithm	SSL	TCP(3389): sha256WithRSAEncryption
SSL Certificate Subject	SSL	TCP(3389): commonName=WE7VMESEIHP001.myl.com
SSL Certificate Valid From	SSL	TCP(3389): Wed Sep 11 11:31:21 2024 UTC
SSL Certificate Valid To	SSL	TCP(3389): Thu Mar 13 11:31:21 2025 UTC
SSL/TLS Enabled Ciphers	SSL	TCP(3389) TLSv1.1: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA\, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA\, TLS_RSA_WITH_AES_256_CBC_SHA\, TLS_RSA_WITH_AES_128_CBC_SHA; TCP(3389) TLSv1: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA\, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA\, TLS_RSA_WITH_AES_256_CBC_SHA\, TLS_RSA_WITH_AES_128_CBC_SHA; TCP(3389) TLSv1.2: 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\, 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;
TLSv1 CBC Ciphers	SSL	The following CBC ciphers are supported on TCP(3389): TLS_RSA_WITH_AES_128_CBC_SHA (128-bit)\, TLS_RSA_WITH_AES_256_CBC_SHA (256-bit)\, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (128-bit)\, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (256-bit)
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)
WDRT Authentication Success	TCP	False
WDRT_Access	TCP	WDRT_SMB_AUTH_SUCCESS : False, WDRT_SMB_REGISTRY_ACCESS : False, WDRT_SMB_FILE_ACCESS : False, WDRT_RPC_AUTH_SUCCESS : False, WDRT_WMI_AUTH_SUCCESS : False, WDRT_HOST_IS_64BIT : False,

Vulnerabilities

Vulnerability	CVE	Hosts	Score
DCE RPC mapper available		1	0
NetBIOS SSN Available		1	0
SMB AUTHENTICATION FAILURE		1	0
RPC DCOM AUTHENTICATION FAILURE		1	0
WMI AUTHENTICATION FAILURE		1	0
Microsoft Remote Desktop Service Available		1	0
IP Addresses Enumerated Via NetBIOS		1	0
SSL Server Supports CBC Ciphers for TLSv1 Encrypted RDP Sessions		1	0

Vulnerability

Vulnerability Name	DCE RPC mapper available	**Score**	0
Published		**Strategy**	Network Reconnaissance
	nCircle: 1225	**CVSS v2**	0.0
CVSS v3	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
WE7VMESEIHP001.myl.com	10.4.37.106	0

Vulnerability

Vulnerability Name	NetBIOS SSN Available	**Score**	0
Published		**Strategy**	Access Control Breach
	nCircle: 1492	**CVSS v2**	0.0
CVSS v3	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
WE7VMESEIHP001.myl.com	10.4.37.106	0

Vulnerability

Vulnerability Name	SMB AUTHENTICATION FAILURE	**Score**	0
Published	nCircle: 5452	**Strategy**	Access Control Breach
CVSS v3	0.0	**CVSS v2**	0.0

Description

DESCRIPTION
IP360 was unable to log into a device, making DRT testing impossible 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 host_access & ASPL_WDRT.WDRT_SMB_AUTH_SUCCESS: rule.
STOP( False ) }
```

Hosts

Hostname	IP Address	Score
WE7VMESEIHP001.myl.com	10.4.37.106	0

Vulnerability

Vulnerability Name	RPC DCOM AUTHENTICATION FAILURE	**Score**	0
Published	nCircle: 9972	**Strategy**	Network Reconnaissance
CVSS v3	0.0	**CVSS v2**	0.0

Description

DESCRIPTION
RPC DCOM AUTHENTICATION FAILURE

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_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 host_access & ASPL_WDRT.WDRT_RPC_AUTH_SUCCESS: rule.
STOP( False ) }
```

Hosts

Hostname	IP Address	Score
WE7VMESEIHP001.myl.com	10.4.37.106	0

Vulnerability

Vulnerability Name	WMI AUTHENTICATION FAILURE	**Score**	0
Published		**Strategy**	Network Reconnaissance
	nCircle: 9974	**CVSS v2**	0.0
CVSS v3	0.0		

Description

DESCRIPTION
WMI AUTHENTICATION FAILURE

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_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 host_access & ASPL_WDRT.WDRT_WMI_AUTH_SUCCESS: rule.
STOP( False ) }
```

Hosts

Hostname	IP Address	Score
WE7VMESEIHP001.myl.com	10.4.37.106	0

Vulnerability

Vulnerability Name	Microsoft Remote Desktop Service Available	**Score**	0
Published		**Strategy**	Network Reconnaissance
	nCircle: 27350	**CVSS v2**	0.0
CVSS v3	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
WE7VMESEIHP001.myl.com	10.4.37.106	0

Vulnerability

Vulnerability Name	IP Addresses Enumerated Via NetBIOS	**Score**	0
Published		**Strategy**	Network Reconnaissance
	nCircle: 28951	**CVSS v2**	0.0
CVSS v3	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’, ’0’ :  ’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
WE7VMESEIHP001.myl.com	10.4.37.106	0

Vulnerability

Vulnerability Name	SSL Server Supports CBC Ciphers for TLSv1 Encrypted RDP Sessions	**Score**	0
Published		**Strategy**	Access Control Breach
	nCircle: 80216	**CVSS v2**	0.0
CVSS v3	0.0		

Description

DESCRIPTION
Cipher Block Chaining (CBC) is vulnerable to beast attacks. BEAST attack relies on a weakness in the way CBC mode is used in SSL and TLS.
SOLUTION
Windows XP and Windows 2003:

Locate the following key in the registry:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL

In the SCHANNEL\Ciphers\RC2 56/56 Subkey, change the DWORD value data of the Enabled value to 0x0. If the Enabled value does not exist, create it.

In the SCHANNEL\Ciphers\RC2 40/128 Subkey, change the DWORD value data of the Enabled value to 0x0. If the Enabled value does not exist, create it.

In the SCHANNEL\Ciphers\DES 168/168 Subkey, change the DWORD value data of the Enabled value to 0x0. If the Enabled value does not exist, create it.

See http://support.microsoft.com/kb/245030 for more information.

Windows Vista, Windows 2008, Windows 7, Windows 2008 R2, Windows 8 and Windows 2012

1. Open Group Policy Manager (gpmc.msc) or Group Policy Editor (gpedit.msc)

2. Select a policy to edit

3. Navigate to <Policy>\Computer Configuration\Policies\Administrative Template\Network\SSL Configuration

4. Right click SSL Cipher Suite Order and click Edit

5. Select Enable

6. Copy the list of SSL Cipher Suites to a text editor

7. Remove unwanted ciphers from the list

continued on next page

8. Paste the updated cipher list back into the SSL Cipher Suites box

9. Click Apply

10. Restart the system (This is necessary as the ciphers are still enabled until a reboot.)

See http://msdn.microsoft.com/en-us/library/bb870930(v=vs.85).aspx for more information.

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

```
EXECUTE{ import HIC, aspl_env, dp try:  all_accepted_ciphers = aspl_env.getContextVariable(’ssl_ciphers’) e
xcept KeyError:  rule.STOP(False)
target_protocol = "TLSv1" #CBC Ciphers weak_ciphers = dict() weak_cipher
s[’\x00\x06’] = ’TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (40-bit)’ weak_ciphers[’\x00\x07’] = ’TLS_RSA_WITH_IDEA_CB
C_SHA (128-bit)’ weak_ciphers[’\x00\x08’] = ’TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (40-bit)’ weak_ciphers[’\x00\x0
9’] = ’TLS_RSA_WITH_DES_CBC_SHA (56-bit)’ weak_ciphers[’\x00\x0a’] = ’TLS_RSA_WITH_3DES_EDE_CBC_SHA (192-bit)’
weak_ciphers[’\x00\x0b’] = ’TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA (40-bit)’ weak_ciphers[’\x00\x0c’] = ’TLS_DH
_DSS_WITH_DES_CBC_SHA (56-bit)’ weak_ciphers[’\x00\x0e’] = ’TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA (40-bit)’ wea
k_ciphers[’\x00\x0f’] = ’TLS_DH_RSA_WITH_DES_CBC_SHA (56-bit)’ weak_ciphers[’\x00\x10’] = ’TLS_DH_RSA_WITH_3DE
S_EDE_CBC_SHA (168-bit)’ weak_ciphers[’\x00\x11’] = ’TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA (40-bit)’ weak_ciph
...
```

Hosts

Hostname	IP Address	Score
WE7VMESEIHP001.myl.com	10.4.37.106	0

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 1809 Direct SMB Session Service	1
IPv4 Layer 4		1
Microsoft Remote Desktop Protocol		1
NetBIOS Name Service	Windows NetBIOS Name Service	1
NetBIOS Session Service	Microsoft Windows OS Family 1809 NetBIOS Session Service	1
Open TCP Port	N/A	1
SMB-Auth	N/A	1

Audits

Network Name	Scan Profile Name	Audit Start	Audit End	Approx Hours Taken
A_AHS_Scan4_NoSIH	_Mylan: Standard Profile	09/13/2024 06:07	09/13/2024 06:09	00:01