Scan Report

April 30, 2023

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "widows-server-first-scan". The scan started at Sun Apr 30 19:09:42 2023 UTC and ended at Sun Apr 30 19:24:25 2023 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview **2**

2 Results per Host **2**

2.1 192.168.145.129 2

2.1.1 High 445/tcp 2

2.1.2 High 3389/tcp 4

2.1.3 High 3050/tcp 5

2.1.4 High 80/tcp 6

2.1.5 Medium 21/tcp 7

2.1.6 Medium 3389/tcp 9

2.1.7 Medium 135/tcp 13

2.1.8 Medium 80/tcp 15

2.1.9 Low general/tcp 16

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.145.129 king-arthur	4	6	1	0	0
Total: 1	4	6	1	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 11 results selected by the filtering described above. Before filtering there were 57 results.

2 Results per Host

2.1 192.168.145.129

Host scan start	Sun Apr 30 19:10:33 2023 UTC
Host scan end	Sun Apr 30 19:24:23 2023 UTC

Service (Port)	Threat Level
445/tcp	High
3389/tcp	High
3050/tcp	High
80/tcp	High
21/tcp	Medium
3389/tcp	Medium
135/tcp	Medium
80/tcp	Medium
general/tcp	Low

2.1.1 High 445/tcp

High (CVSS: 9.3)
NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012 R2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Service Pack 2

Vulnerability Insight
Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

Vulnerability Detection Method
Send the crafted SMB transaction request with fid = 0 and check the response to confirm the vulnerability.
Details: `Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)`
OID:1.3.6.1.4.1.25623.1.0.810676
Version used: `2020-06-04T12:11:49Z`

References
`cve: CVE-2017-0143`
`cve: CVE-2017-0144`
`cve: CVE-2017-0145`
`cve: CVE-2017-0146`
`cve: CVE-2017-0147`
`cve: CVE-2017-0148`
`bid: 96703`

. . . continues on next page . . .

... continued from previous page ...

```
bid: 96704
bid: 96705
bid: 96707
bid: 96709
bid: 96706
url: https://support.microsoft.com/en-in/kb/4013078
url: https://technet.microsoft.com/library/security/MS17-010
url: https://github.com/rapid7/metasploit-framework/pull/8167/files
cert-bund: CB-K17/0435
dfn-cert: DFN-CERT-2017-0448
```

[return to 192.168.145.129]

2.1.2 High 3389/tcp

High (CVSS: 10.0)
NVT: Microsoft Windows Remote Desktop Services 'CVE-2019-0708' Remote Code Execution Vulnerability (BlueKeep) - (Remote Active)

Summary
This host is running Microsoft Windows Remote Desktop Services and is prone to the remote code execution vulnerability known as 'BlueKeep'.

Vulnerability Detection Result
```
By sending a crafted request the RDP service answered with a 'MCS Disconnect Pro
↪vider Ultimatum PDU - 2.2.2.3' response which indicates that a RCE attack can
↪be executed.
```

Impact
Successful exploitation would allow an attacker to execute arbitrary code on the target system. An attacker could then install programs, view, change, or delete data, or create new accounts with full user rights.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.
As a workaround enable Network Level Authentication (NLA) on systems running supported editions of Windows 7, Windows Server 2008, and Windows Server 2008 R2.
NOTE: After enabling NLA affected systems are still vulnerable to Remote Code Execution (RCE) exploitation if the attacker has valid credentials that can be used to successfully authenticate.

Affected Software/OS
- Microsoft Windows 7
- Microsoft Windows Server 2008 R2

... continues on next page ...

... continued from previous page ...

- Microsoft Windows Server 2008
- Microsoft Windows Server 2003 R2
- Microsoft Windows Server 2003
- Microsoft Windows Vista and Microsoft Windows XP (including Embedded)

Vulnerability Insight
A remote code execution vulnerability exists in Remote Desktop Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction.
For an in-depth analysis and further technical insights and details please see the references.

Vulnerability Detection Method
Sends a specially crafted request to the target systems Remote Desktop Service via RDP and checks the response.
Details: `Microsoft Windows Remote Desktop Services 'CVE-2019-0708' Remote Code Execution. ↪..`
OID:1.3.6.1.4.1.25623.1.0.108611
Version used: `2020-11-10T09:46:51Z`

References
`cve: CVE-2019-0708`
`bid: 108273`
`url: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019 ↪-0708`
`url: https://support.microsoft.com/help/4499164`
`url: https://support.microsoft.com/help/4499175`
`url: https://support.microsoft.com/help/4499149`
`url: https://support.microsoft.com/help/4499180`
`url: https://support.microsoft.com/help/4500331`
`url: https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updat ↪ing-remote-desktop-services-cve-2019-0708/`
`url: https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve- ↪2019-0708`
`url: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-s ↪erver-2008-R2-and-2008/cc732713(v=ws.11)`
`url: http://www.securityfocus.com/bid/108273`
`url: http://packetstormsecurity.com/files/153133/Microsoft-Windows-Remote-Deskto ↪p-BlueKeep-Denial-Of-Service.html`
`url: https://www.malwaretech.com/2019/05/analysis-of-cve-2019-0708-bluekeep.html`
`url: https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/rdp-stands-for- ↪really-do-patch-understanding-the-wormable-rdp-vulnerability-cve-2019-0708`
`cert-bund: CB-K19/0415`
`dfn-cert: DFN-CERT-2019-0977`

[return to 192.168.145.129]

2.1.3 High 3050/tcp

High (CVSS: 9.0)
NVT: Firebird Default Credentials

Summary
It is possible to connect to the remote database service using default credentials.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
An attacker may use this flaw to execute commands against the remote host, as well as read your database content.

Solution:
Solution type: Mitigation
Change the default password by using the gsec management tool.

Vulnerability Insight
The remote Firebird Server uses default credentials (SYSDBA/masterkey).

Vulnerability Detection Method
Details: `Firebird Default Credentials`
OID:1.3.6.1.4.1.25623.1.0.100792
Version used: `2020-11-10T09:46:51Z`

References
`url: http://www.firebirdsql.org/manual/qsg2-config.html#qsg2-config-security`

[return to 192.168.145.129]

2.1.4 High 80/tcp

High (CVSS: 10.0)
NVT: MS15-034 HTTP.sys Remote Code Execution Vulnerability (Active Check)

Product detection result
`cpe:/a:microsoft:internet_information_services:7.5`
`Detected by Microsoft Internet Information Services (IIS) Detection (HTTP) (OID:`
`↪ 1.3.6.1.4.1.25623.1.0.900710)`

Summary
This host is missing an important security update according to Microsoft Bulletin MS15-034.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

. . . continues on next page . . .

... continued from previous page ...

Impact
Successful exploitation will allow remote attackers to run arbitrary code in the context of the current user and to perform actions in the security context of the current user.

Solution:
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

Affected Software/OS
- Microsoft Windows 8 x32/x64
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2008 x32/x64 Service Pack 2 and prior
- Microsoft Windows 7 x32/x64 Service Pack 1 and prior

Vulnerability Insight
Flaw exists due to the HTTP protocol stack 'HTTP.sys' that is triggered when parsing HTTP requests.

Vulnerability Detection Method
Send a special crafted HTTP GET request and check the response
Details: `MS15-034 HTTP.sys Remote Code Execution Vulnerability (Active Check)`
OID:1.3.6.1.4.1.25623.1.0.105257
Version used: `2020-11-25T11:26:55Z`

Product Detection Result
Product: `cpe:/a:microsoft:internet_information_services:7.5`
Method: `Microsoft Internet Information Services (IIS) Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.900710)

References
`cve: CVE-2015-1635`
`url: https://support.microsoft.com/kb/3042553`
`url: https://technet.microsoft.com/library/security/MS15-034`
`url: http://pastebin.com/ypURDPc4`
`cert-bund: CB-K15/0527`
`dfn-cert: DFN-CERT-2015-0545`

[return to 192.168.145.129]

2.1.5 Medium 21/tcp

Medium (CVSS: 6.4)
NVT: Anonymous FTP Login Reporting

Summary
Reports if the remote FTP Server allows anonymous logins.

Vulnerability Detection Result
```
It was possible to login to the remote FTP service with the following anonymous
↪account(s):
anonymous:anonymous@example.com
Here are the contents of the remote FTP directory listing:
Account "anonymous":
drwxr-xr-x 1 ftp ftp              0 Jul 16  2020 aspnet_client
-rw-r--r-- 1 ftp ftp            689 Jul 16  2020 iisstart.htm
-rw-r--r-- 1 ftp ftp         184946 Jul 16  2020 welcome.png
```

Impact
Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to:
- gain access to sensitive files
- upload or delete files.

Solution:
Solution type: Mitigation
If you do not want to share files, you should disable anonymous logins.

Vulnerability Insight
A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.

Vulnerability Detection Method
Details: `Anonymous FTP Login Reporting`
OID:1.3.6.1.4.1.25623.1.0.900600
Version used: `2020-08-24T08:40:10Z`

References
`url: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497`

Medium (CVSS: 4.8)
NVT: FTP Unencrypted Cleartext Login

Summary

. . . continues on next page . . .

... continued from previous page ...

The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Vulnerability Detection Result

```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Non-anonymous sessions: 331 Password required for openvasvt
Anonymous sessions:     331 Password required for anonymous
```

Impact

An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution:

Solution type: Mitigation

Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Vulnerability Detection Method

Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.

Details: `FTP Unencrypted Cleartext Login`

OID:1.3.6.1.4.1.25623.1.0.108528

Version used: `2020-08-24T08:40:10Z`

[return to 192.168.145.129]

2.1.6 Medium 3389/tcp

Medium (CVSS: 5.0)
NVT: SSL/TLS: Report Weak Cipher Suites

Summary

This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Vulnerability Detection Result

```
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
```

Solution:

Solution type: Mitigation

... continues on next page ...

... continued from previous page ...

The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.
Please see the references for more resources supporting you with this task.

Vulnerability Insight
These rules are applied for the evaluation of the cryptographic strength:
- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808).
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000).
- 1024 bit RSA authentication is considered to be insecure and therefore as weak.
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

Vulnerability Detection Method
Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2020-11-26T08:02:59Z

References
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/
url: https://mozilla.github.io/server-side-tls/ssl-config-generator/
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334

... continues on next page ...

... continued from previous page ...

cert-bund: CB-K15/1269
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
dfn-cert: DFN-CERT-2015-1341

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

Medium (CVSS: 4.0)
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm

Summary
The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result

```
The following certificates are part of the certificate chain but using insecure
↪signature algorithms:
Subject:              CN=king-arthur
Signature Algorithm:  sha1WithRSAEncryption
```

Solution:
Solution type: Mitigation
Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:
- Secure Hash Algorithm 1 (SHA-1)
- Message Digest 5 (MD5)
- Message Digest 4 (MD4)
- Message Digest 2 (MD2)
Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.
NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:
Fingerprint1
or
fingerprint1,Fingerprint2

Vulnerability Detection Method
Check which hashing algorithm was used to sign the remote SSL/TLS certificate.
Details: `SSL/TLS: Certificate Signed Using A Weak Signature Algorithm`
OID:1.3.6.1.4.1.25623.1.0.105880
Version used: `2021-02-18T11:08:41Z`

References
`url: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/`

[return to 192.168.145.129]

2.1.7 Medium 135/tcp

Medium (CVSS: 5.0)
NVT: DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Vulnerability Detection Result
```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49152/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.145.129[49152]
Port: 49153/tcp
     UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
```

... continues on next page ...

... continued from previous page ...

```
      Endpoint: ncacn_ip_tcp:192.168.145.129[49153]
      Annotation: NRP server endpoint
      UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
      Endpoint: ncacn_ip_tcp:192.168.145.129[49153]
      Annotation: DHCP Client LRPC Endpoint
      UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
      Endpoint: ncacn_ip_tcp:192.168.145.129[49153]
      Annotation: DHCPv6 Client LRPC Endpoint
      UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
      Endpoint: ncacn_ip_tcp:192.168.145.129[49153]
      Annotation: Event log TCPIP
Port: 49154/tcp
      UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1
      Endpoint: ncacn_ip_tcp:192.168.145.129[49154]
      UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
      Endpoint: ncacn_ip_tcp:192.168.145.129[49154]
      Annotation: IP Transition Configuration endpoint
      UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
      Endpoint: ncacn_ip_tcp:192.168.145.129[49154]
      UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
      Endpoint: ncacn_ip_tcp:192.168.145.129[49154]
      Annotation: XactSrv service
      UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
      Endpoint: ncacn_ip_tcp:192.168.145.129[49154]
      Annotation: IKE/Authip API
      UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
      Endpoint: ncacn_ip_tcp:192.168.145.129[49154]
      Annotation: Impl friendly name
Port: 49155/tcp
      UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
      Endpoint: ncacn_ip_tcp:192.168.145.129[49155]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access
Port: 49160/tcp
      UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
      Endpoint: ncacn_ip_tcp:192.168.145.129[49160]
Port: 49163/tcp
      UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
      Endpoint: ncacn_ip_tcp:192.168.145.129[49163]
      Annotation: IPSec Policy agent endpoint
      Named pipe : spoolss
      Win32 service or process : spoolsv.exe
      Description : Spooler service
      UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
      Endpoint: ncacn_ip_tcp:192.168.145.129[49163]
      Annotation: Remote Fw APIs
```

... continues on next page ...

... continued from previous page ...

Note: DCE/RPC or MSRPC services running on this host locally were identified. Re
↪porting this list is not enabled by default due to the possible large size of
↪this list. See the script preferences to enable this reporting.

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution:
Solution type: Mitigation
Filter incoming traffic to this ports.

Vulnerability Detection Method
Details: DCE/RPC and MSRPC Services Enumeration Reporting
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: 2017-06-13T07:06:12Z

[return to 192.168.145.129]

2.1.8 Medium 80/tcp

Medium (CVSS: 5.0)
NVT: Microsoft IIS Default Welcome Page Information Disclosure Vulnerability

Product detection result
cpe:/a:microsoft:internet_information_services:7.5
Detected by Microsoft Internet Information Services (IIS) Detection (HTTP) (OID:
↪ 1.3.6.1.4.1.25623.1.0.900710)

Summary
The host is running Microsoft IIS Webserver and is prone to information disclosure vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow remote attackers to obtain sensitive information that could aid in further attacks.

Solution:
Solution type: Mitigation
Disable the default pages within the server configuration.

Affected Software/OS

... continues on next page ...

... continued from previous page ...

Microsoft Internet Information Services.

Vulnerability Insight
The flaw is due to misconfiguration of IIS Server, which allows to access default pages when the server is not used.

Vulnerability Detection Method
Details: `Microsoft IIS Default Welcome Page Information Disclosure Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.802806
Version used: `2020-11-25T11:26:55Z`

Product Detection Result
Product: `cpe:/a:microsoft:internet_information_services:7.5`
Method: `Microsoft Internet Information Services (IIS) Detection (HTTP)`
OID: 1.3.6.1.4.1.25623.1.0.900710)

[return to 192.168.145.129]

2.1.9 Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 175095
Packet 2: 175183
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution:
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'
Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP timestamps`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2020-08-24T08:40:10Z`

References
`url: http://www.ietf.org/rfc/rfc1323.txt`
`url: http://www.ietf.org/rfc/rfc7323.txt`
`url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d`
`↪ownload/details.aspx?id=9152`

[return to 192.168.145.129]