Delta Report

April 23, 2025

Delta Report Summary

This document compares the results of two security scans. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Server2025". The first scan started at Sun Apr 20 01:26:22 2025 UTC and ended at 2025-04-20T02:14:21Z. The second scan started at Sun Apr 20 19:22:07 2025 UTC and ended at Sun Apr 20 20:11:05 2025 UTC. The report first summarises the hosts found. Then, for each host, the report describes the changes that occurred between the two scans.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.1.2	0	2	2	0	0
Total: 1	0	2	2	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 4 results selected by the filtering described above.

2 Results per Host

2.1 192.168.1.2

Host scan start	Sun Apr 20 01:28:25 2025 UTC
Host scan end	Sun Apr 20 02:14:16 2025 UTC

Service (Port)	Threat Level
3389/tcp	Medium
135/tcp	Medium
22/tcp	Low
general/tcp	Low

2.1.1 Medium 3389/tcp

= Medium (CVSS: 4.3)

NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Product detection result
`cpe:/a:ietf:transport_layer_security:1.0`
`Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)`

... continues on next page ...

... continued from previous page ...

Summary
It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Quality of Detection (QoD): 98%

Vulnerability Detection Result
`In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and ↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c ↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1 ↪.25623.1.0.802067) VT.`

Impact
An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.
Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:
Solution type: Mitigation
It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

Affected Software/OS
All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols.

Vulnerability Insight
The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:
- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method
Check the used TLS protocols of the services provided by this system.
Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.117274
Version used: `2024-09-27T05:05:23Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security:1.0`
Method: `SSL/TLS: Version Detection`
OID: 1.3.6.1.4.1.25623.1.0.105782)

... continues on next page ...

... continued from previous page ...

References

cve: CVE-2011-3389
cve: CVE-2015-0204
url: https://ssl-config.mozilla.org/
url: https://bettercrypto.org/
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800

... continues on next page ...

... continued from previous page ...

dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123

... continues on next page ...

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

[return to 192.168.1.2]

2.1.2 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.

Quality of Detection (QoD): 80%

Result 1

Vulnerability Detection Result

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49664/tcp
     UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
     Endpoint: ncacn_ip_tcp:192.168.1.2[49664]
     Annotation: RemoteAccessCheck
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.2[49664]
     Named pipe : lsass
     Win32 service or process : lsass.exe
```

... continues on next page ...

... continued from previous page ...

```
      Description : SAM access
      UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49664]
      Annotation: Ngc Pop Key Service
      UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49664]
      Annotation: Ngc Pop Key Service
      UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
      Endpoint: ncacn_ip_tcp:192.168.1.2[49664]
      Annotation: KeyIso
      UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49664]
      Annotation: Impl friendly name
Port: 49665/tcp
      UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49665]
Port: 49666/tcp
      UUID: 89759fce-5a25-4086-8967-de12f39a60b5, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49666]
      UUID: 9b3195fe-d603-43d1-a0d5-9072d7cde122, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49666]
Port: 49667/tcp
      UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49667]
      UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49667]
Port: 49669/tcp
      UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
      Endpoint: ncacn_ip_tcp:192.168.1.2[49669]
      Annotation: RemoteAccessCheck
      UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49669]
      Annotation: Impl friendly name
Port: 49671/tcp
      UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49671]
      UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49671]
      Named pipe : spoolss
      Win32 service or process : spoolsv.exe
      Description : Spooler service
      UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49671]
      UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49671]
      UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49671]
```

... continues on next page ...

... continued from previous page ...

```
Port: 49672/tcp
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.2[49672]
     Annotation: Windows Event Log
Port: 49673/tcp
     UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.2[49673]
Port: 49680/tcp
     UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
     Endpoint: ncacn_ip_tcp:192.168.1.2[49680]
     Annotation: RemoteAccessCheck
     UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
     Endpoint: ncacn_ip_tcp:192.168.1.2[49680]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : LSA access
     UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
     Endpoint: ncacn_ip_tcp:192.168.1.2[49680]
     Annotation: MS NT Directory DRS Interface
Port: 49681/tcp
     UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
     Endpoint: ncacn_http:192.168.1.2[49681]
     Annotation: RemoteAccessCheck
     UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
     Endpoint: ncacn_http:192.168.1.2[49681]
     Named pipe : lsass
     Win32 service or process : Netlogon
     Description : Net Logon service
     UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
     Endpoint: ncacn_http:192.168.1.2[49681]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : LSA access
     UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
     Endpoint: ncacn_http:192.168.1.2[49681]
     Annotation: MS NT Directory DRS Interface
Port: 49685/tcp
     UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
     Endpoint: ncacn_ip_tcp:192.168.1.2[49685]
     Annotation: 50000
Port: 49696/tcp
     UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.2[49696]
     Named pipe : lsass
     Win32 service or process : Netlogon
     Description : Net Logon service
Port: 49698/tcp
```

... continues on next page ...

... continued from previous page ...

```
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:192.168.1.2[49698]
Port: 49699/tcp
     UUID: 32e36e84-4ba2-496c-ba85-fb450f325107, version 2
     Endpoint: ncacn_ip_tcp:192.168.1.2[49699]
     UUID: aa177641-fc9b-41bd-80ff-f964a701596f, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.2[49699]
     UUID: c95fc993-f460-4763-a00d-bb3b9e5c7e2e, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.2[49699]
Port: 49709/tcp
     UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5
     Endpoint: ncacn_ip_tcp:192.168.1.2[49709]
     Named pipe : dnsserver
     Win32 service or process : dns.exe
     Description : DNS Server
Port: 5504/tcp
     UUID: ed96b012-c8ce-4f60-a682-35535b12ff75, version 2
     Endpoint: ncacn_ip_tcp:192.168.1.2[5504]
Port: 56746/tcp
     UUID: 897e2e5f-93f3-4376-9c9c-fd2277495c27, version 1
     Endpoint: ncacn_ip_tcp:192.168.1.2[56746]
     Annotation: Frs2 Service
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: 2022-06-03T10:17:07Z

Result 2

```
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP p
↪rotocol:
Port: 49664/tcp
     UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
     Endpoint: ncacn_ip_tcp:192.168.1.2[49664]
     Annotation: RemoteAccessCheck
```

... continues on next page ...

... continued from previous page ...

```
      UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49664]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : SAM access
      UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49664]
      Annotation: Ngc Pop Key Service
      UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49664]
      Annotation: Ngc Pop Key Service
      UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
      Endpoint: ncacn_ip_tcp:192.168.1.2[49664]
      Annotation: KeyIso
      UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49664]
      Annotation: Impl friendly name
Port: 49665/tcp
      UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49665]
Port: 49666/tcp
      UUID: 89759fce-5a25-4086-8967-de12f39a60b5, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49666]
      UUID: 9b3195fe-d603-43d1-a0d5-9072d7cde122, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49666]
Port: 49667/tcp
      UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49667]
      Annotation: Windows Event Log
Port: 49668/tcp
      UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49668]
      UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49668]
Port: 49670/tcp
      UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49670]
      UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49670]
      Named pipe : spoolss
      Win32 service or process : spoolsv.exe
      Description : Spooler service
      UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49670]
      UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49670]
      UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
```

... continues on next page ...

... continued from previous page ...

```
      Endpoint: ncacn_ip_tcp:192.168.1.2[49670]
Port: 49671/tcp
      UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
      Endpoint: ncacn_ip_tcp:192.168.1.2[49671]
      Annotation: RemoteAccessCheck
      UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49671]
      Annotation: Impl friendly name
Port: 49673/tcp
      UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49673]
Port: 49684/tcp
      UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
      Endpoint: ncacn_ip_tcp:192.168.1.2[49684]
      Annotation: RemoteAccessCheck
      UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
      Endpoint: ncacn_ip_tcp:192.168.1.2[49684]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : LSA access
      UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
      Endpoint: ncacn_ip_tcp:192.168.1.2[49684]
      Annotation: MS NT Directory DRS Interface
Port: 49685/tcp
      UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
      Endpoint: ncacn_http:192.168.1.2[49685]
      Annotation: RemoteAccessCheck
      UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
      Endpoint: ncacn_http:192.168.1.2[49685]
      Named pipe : lsass
      Win32 service or process : Netlogon
      Description : Net Logon service
      UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
      Endpoint: ncacn_http:192.168.1.2[49685]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : LSA access
      UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
      Endpoint: ncacn_http:192.168.1.2[49685]
      Annotation: MS NT Directory DRS Interface
Port: 49689/tcp
      UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
      Endpoint: ncacn_ip_tcp:192.168.1.2[49689]
      Annotation: 50000
Port: 49700/tcp
      UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49700]
```

... continues on next page ...

... continued from previous page ...

```
      Named pipe : lsass
      Win32 service or process : Netlogon
      Description : Net Logon service
Port: 49701/tcp
      UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
      Endpoint: ncacn_ip_tcp:192.168.1.2[49701]
Port: 49702/tcp
      UUID: 32e36e84-4ba2-496c-ba85-fb450f325107, version 2
      Endpoint: ncacn_ip_tcp:192.168.1.2[49702]
      UUID: aa177641-fc9b-41bd-80ff-f964a701596f, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49702]
      UUID: c95fc993-f460-4763-a00d-bb3b9e5c7e2e, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[49702]
Port: 49713/tcp
      UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5
      Endpoint: ncacn_ip_tcp:192.168.1.2[49713]
      Named pipe : dnsserver
      Win32 service or process : dns.exe
      Description : DNS Server
Port: 51376/tcp
      UUID: 897e2e5f-93f3-4376-9c9c-fd2277495c27, version 1
      Endpoint: ncacn_ip_tcp:192.168.1.2[51376]
      Annotation: Frs2 Service
Port: 5504/tcp
      UUID: ed96b012-c8ce-4f60-a682-35535b12ff75, version 2
      Endpoint: ncacn_ip_tcp:192.168.1.2[5504]
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.
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.10736

Different Lines

```
@@ -43,139 +43,139 @@

 Port: 49667/tcp

-      UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
+      UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
       Endpoint: ncacn_ip_tcp:192.168.1.2[49667]
-      Annotation: Windows Event Log

-Port: 49668/tcp
+      UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
```

... continues on next page ...

... continued from previous page ...

```
+      Endpoint: ncacn_ip_tcp:192.168.1.2[49667]

-      UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
-      Endpoint: ncacn_ip_tcp:192.168.1.2[49668]
+Port: 49669/tcp

-      UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
-      Endpoint: ncacn_ip_tcp:192.168.1.2[49668]
+      UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
+      Endpoint: ncacn_ip_tcp:192.168.1.2[49669]
+      Annotation: RemoteAccessCheck

-Port: 49670/tcp
+      UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
+      Endpoint: ncacn_ip_tcp:192.168.1.2[49669]
+      Annotation: Impl friendly name
+
+Port: 49671/tcp

       UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
-      Endpoint: ncacn_ip_tcp:192.168.1.2[49670]
+      Endpoint: ncacn_ip_tcp:192.168.1.2[49671]

       UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
-      Endpoint: ncacn_ip_tcp:192.168.1.2[49670]
+      Endpoint: ncacn_ip_tcp:192.168.1.2[49671]
       Named pipe : spoolss
       Win32 service or process : spoolsv.exe
       Description : Spooler service

       UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
-      Endpoint: ncacn_ip_tcp:192.168.1.2[49670]
+      Endpoint: ncacn_ip_tcp:192.168.1.2[49671]

       UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
-      Endpoint: ncacn_ip_tcp:192.168.1.2[49670]
+      Endpoint: ncacn_ip_tcp:192.168.1.2[49671]

       UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
-      Endpoint: ncacn_ip_tcp:192.168.1.2[49670]
-
-Port: 49671/tcp
-
-      UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
       Endpoint: ncacn_ip_tcp:192.168.1.2[49671]
-      Annotation: RemoteAccessCheck
```

... continues on next page ...

... continued from previous page ...

```
-      UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
-      Endpoint: ncacn_ip_tcp:192.168.1.2[49671]
-      Annotation: Impl friendly name
+Port: 49672/tcp
+
+      UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
+      Endpoint: ncacn_ip_tcp:192.168.1.2[49672]
+      Annotation: Windows Event Log

 Port: 49673/tcp

       UUID: 29770a8f-829b-4158-90a2-78cd488501f7, version 1
       Endpoint: ncacn_ip_tcp:192.168.1.2[49673]

-Port: 49684/tcp
+Port: 49680/tcp

       UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
-      Endpoint: ncacn_ip_tcp:192.168.1.2[49684]
+      Endpoint: ncacn_ip_tcp:192.168.1.2[49680]
       Annotation: RemoteAccessCheck

       UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
-      Endpoint: ncacn_ip_tcp:192.168.1.2[49684]
+      Endpoint: ncacn_ip_tcp:192.168.1.2[49680]
       Named pipe : lsass
       Win32 service or process : lsass.exe
       Description : LSA access

       UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
-      Endpoint: ncacn_ip_tcp:192.168.1.2[49684]
+      Endpoint: ncacn_ip_tcp:192.168.1.2[49680]
       Annotation: MS NT Directory DRS Interface

-Port: 49685/tcp
+Port: 49681/tcp

       UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
-      Endpoint: ncacn_http:192.168.1.2[49685]
+      Endpoint: ncacn_http:192.168.1.2[49681]
       Annotation: RemoteAccessCheck

       UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
-      Endpoint: ncacn_http:192.168.1.2[49685]
+      Endpoint: ncacn_http:192.168.1.2[49681]
       Named pipe : lsass
       Win32 service or process : Netlogon
```

... continues on next page ...

... continued from previous page ...

```
      Description : Net Logon service

      UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
-     Endpoint: ncacn_http:192.168.1.2[49685]
+     Endpoint: ncacn_http:192.168.1.2[49681]
      Named pipe : lsass
      Win32 service or process : lsass.exe
      Description : LSA access

      UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
-     Endpoint: ncacn_http:192.168.1.2[49685]
+     Endpoint: ncacn_http:192.168.1.2[49681]
      Annotation: MS NT Directory DRS Interface

-Port: 49689/tcp
+Port: 49685/tcp

      UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
-     Endpoint: ncacn_ip_tcp:192.168.1.2[49689]
+     Endpoint: ncacn_ip_tcp:192.168.1.2[49685]
      Annotation: 50000

-Port: 49700/tcp
+Port: 49696/tcp

      UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
-     Endpoint: ncacn_ip_tcp:192.168.1.2[49700]
+     Endpoint: ncacn_ip_tcp:192.168.1.2[49696]
      Named pipe : lsass
      Win32 service or process : Netlogon
      Description : Net Logon service

-Port: 49701/tcp
+Port: 49698/tcp

      UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
-     Endpoint: ncacn_ip_tcp:192.168.1.2[49701]
+     Endpoint: ncacn_ip_tcp:192.168.1.2[49698]

-Port: 49702/tcp
+Port: 49699/tcp

      UUID: 32e36e84-4ba2-496c-ba85-fb450f325107, version 2
-     Endpoint: ncacn_ip_tcp:192.168.1.2[49702]
+     Endpoint: ncacn_ip_tcp:192.168.1.2[49699]

      UUID: aa177641-fc9b-41bd-80ff-f964a701596f, version 1
```

... continues on next page ...

... continued from previous page ...

```
-      Endpoint: ncacn_ip_tcp:192.168.1.2[49702]
+      Endpoint: ncacn_ip_tcp:192.168.1.2[49699]

       UUID: c95fc993-f460-4763-a00d-bb3b9e5c7e2e, version 1
-      Endpoint: ncacn_ip_tcp:192.168.1.2[49702]
+      Endpoint: ncacn_ip_tcp:192.168.1.2[49699]

-Port: 49713/tcp
+Port: 49709/tcp

       UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5
-      Endpoint: ncacn_ip_tcp:192.168.1.2[49713]
+      Endpoint: ncacn_ip_tcp:192.168.1.2[49709]
       Named pipe : dnsserver
       Win32 service or process : dns.exe
       Description : DNS Server

-Port: 51376/tcp
-
-      UUID: 897e2e5f-93f3-4376-9c9c-fd2277495c27, version 1
-      Endpoint: ncacn_ip_tcp:192.168.1.2[51376]
-      Annotation: Frs2 Service
-
 Port: 5504/tcp

       UUID: ed96b012-c8ce-4f60-a682-35535b12ff75, version 2
       Endpoint: ncacn_ip_tcp:192.168.1.2[5504]

+Port: 56746/tcp
+
+      UUID: 897e2e5f-93f3-4376-9c9c-fd2277495c27, version 1
+      Endpoint: ncacn_ip_tcp:192.168.1.2[56746]
+      Annotation: Frs2 Service
+
 Note: DCE/RPC or MSRPC services running on this host locally were identified. R
↪eporting this list is not enabled by default due to the possible large size of
↪ this list. See the script preferences to enable this reporting.
```

[return to 192.168.1.2]

2.1.3 Low 22/tcp

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

Product detection result
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565)

Summary
The remote SSH server is configured to allow / support weak MAC algorithm(s).

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The remote SSH server supports the following weak client-to-server MAC algorithm(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm(s):
umac-64-etm@openssh.com
umac-64@openssh.com

Solution:
Solution type: Mitigation
Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm
Details: Weak MAC Algorithm(s) Supported (SSH)
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:secure_shell_protocol
Method: SSH Protocol Algorithms Supported
OID: 1.3.6.1.4.1.25623.1.0.105565)

... continues on next page ...

... continued from previous page ...

References
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4

[return to 192.168.1.2]

2.1.4 Low general/tcp

~ Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

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

Quality of Detection (QoD): 80%

Result 1

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: 804093
Packet 2: 805151

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.

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

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

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 Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-12-15T16:10:08Z`

Result 2

```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 1245538
Packet 2: 1246631
```

OID of test routine: 1.3.6.1.4.1.25623.1.0.80091

Different Lines

```
@@ -1,6 +1,6 @@
 It was detected that the host implements RFC1323/RFC7323.

 The following timestamps were retrieved with a delay of 1 seconds in-between:
-Packet 1: 1245538
-Packet 2: 1246631
+Packet 1: 804093
+Packet 2: 805151
```

References
url: https://datatracker.ietf.org/doc/html/rfc1323
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090

[return to 192.168.1.2]