Scan Report

December 5, 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 “Scan”. The scan started at Tue Dec 5 08:45:23 2023 UTC and ended at Tue Dec 5 09:02:22 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

Host	High	Medium	Low	Log	False Positive
172.16.2.98	1	1	2	0	0
172.16.2.65	1	1	2	0	0
172.16.2.90	1	1	1	0	0
172.16.2.91	0	0	2	0	0
172.16.2.97	0	0	2	0	0
Total: 5	3	3	9	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 15 results selected by the filtering described above. Before filtering there were 86 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
172.16.2.98	SSH	Failure	Protocol SSH, Port 22, User gmarty : Login failure
172.16.2.65	SSH	Failure	Protocol SSH, Port 22, User gmarty : Login failure
172.16.2.90	SSH	Failure	Protocol SSH, Port 22, User gmarty : Login failure
172.16.2.91	SSH	Failure	Protocol SSH, Port 22, User gmarty : Login failure
172.16.2.97	SSH	Failure	Protocol SSH, Port 22, User gmarty : Login failure

2 Results per Host

2.1 172.16.2.98

Host scan start	Tue Dec 5 08:45:59 2023 UTC
Host scan end	Tue Dec 5 08:55:44 2023 UTC

Service (Port)	Threat Level
80/tcp	High

. . . (continues) . . .

. . . (continued) . . .

Service (Port)	Threat Level
80/tcp	Medium
general/icmp	Low
general/tcp	Low

2.1.1 High 80/tcp

High (CVSS: 10.0)
NVT: pfSense Default Admin Credentials (HTTP)

Summary
In pfSense it is possible to gain administrative access via default credentials.

Vulnerability Detection Result

```
It was possible to authenticate with the following credentials:
Username: admin
Password: pfsense
```

Impact
This issue may be exploited by a remote attacker to gain access to sensitive information.

Solution:
Solution type: Mitigation
Change the passwords.

Vulnerability Insight
By convention, each time you create a new instance of pfSense, the admin user is being created with default credentials: Username: admin, Password: pfsense.

Vulnerability Detection Method
Details: `pfSense Default Admin Credentials (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.112122
Version used: `2023-03-01T10:09:26Z`

References

```
url: https://doc.pfsense.org/index.php/Installing_pfSense#pfSense_Default_Config
↪uration
url: https://doc.pfsense.org/index.php/What_is_the_default_username_and_password
```

[return to 172.16.2.98]

2.1.2 Medium 80/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result

```
The following input fields where identified (URL:input name):
http://172.16.2.98/:passwordfld
```

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution:
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2020-08-24T15:18:35Z`

References

```
url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se
↪ssion_Management
url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
url: https://cwe.mitre.org/data/definitions/319.html
```

[return to 172.16.2.98]

2.1.3 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

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

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

Vulnerability Detection Method
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2022-11-18T10:11:40Z`

References
```
cve: CVE-1999-0524
url: http://www.ietf.org/rfc/rfc0792.txt
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[return to 172.16.2.98]

2.1.4 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

. . . continues on next page . . .

. . . continued from previous page . . .

```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 3206934095
Packet 2: 2932428146
```

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

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/download/details.aspx?id=9152

[return to 172.16.2.98]

2.2 172.16.2.65

Host scan start	Tue Dec 5 08:45:59 2023 UTC
Host scan end	Tue Dec 5 08:55:43 2023 UTC

Service (Port)	Threat Level
80/tcp	High
80/tcp	Medium
general/icmp	Low
general/tcp	Low

2.2.1 High 80/tcp

High (CVSS: 10.0)
NVT: pfSense Default Admin Credentials (HTTP)

Summary
In pfSense it is possible to gain administrative access via default credentials.

Vulnerability Detection Result

```
It was possible to authenticate with the following credentials:
Username: admin
Password: pfsense
```

Impact
This issue may be exploited by a remote attacker to gain access to sensitive information.

Solution:
Solution type: Mitigation
Change the passwords.

Vulnerability Insight
By convention, each time you create a new instance of pfSense, the admin user is being created with default credentials: Username: admin, Password: pfsense.

Vulnerability Detection Method
Details: `pfSense Default Admin Credentials (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.112122
Version used: `2023-03-01T10:09:26Z`

References

```
url: https://doc.pfsense.org/index.php/Installing_pfSense#pfSense_Default_Config
↪uration
url: https://doc.pfsense.org/index.php/What_is_the_default_username_and_password
```

[return to 172.16.2.65]

2.2.2 Medium 80/tcp

Medium (CVSS: 4.8)
NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result

```
The following input fields where identified (URL:input name):
http://172.16.2.65/:passwordfld
```

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution:
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2020-08-24T15:18:35Z`

References

```
url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se
↪ssion_Management
url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
url: https://cwe.mitre.org/data/definitions/319.html
```

[return to 172.16.2.65]

2.2.3 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

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

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

Vulnerability Detection Method
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2022-11-18T10:11:40Z`

References
```
cve: CVE-1999-0524
url: http://www.ietf.org/rfc/rfc0792.txt
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[return to 172.16.2.65]

2.2.4 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

. . . continues on next page . . .

. . . continued from previous page . . .

```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 3979896541
Packet 2: 3926387488
```

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

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 172.16.2.65]

2.3 172.16.2.90

Host scan start	Tue Dec 5 08:45:59 2023 UTC
Host scan end	

Service (Port)	Threat Level
445/tcp	High
135/tcp	Medium
general/tcp	Low

2.3.1 High 445/tcp

High (CVSS: 8.1)
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: `2022-08-09T10:11:17Z`

. . . continues on next page . . .

. . . continued from previous page . . .

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
cisa: Known Exploited Vulnerability (KEV) catalog
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
url: https://support.microsoft.com/en-us/kb/4013078
url: http://www.securityfocus.com/bid/96703
url: http://www.securityfocus.com/bid/96704
url: http://www.securityfocus.com/bid/96705
url: http://www.securityfocus.com/bid/96707
url: http://www.securityfocus.com/bid/96709
url: http://www.securityfocus.com/bid/96706
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 172.16.2.90]

2.3.2 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.

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: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49664]
Port: 49665/tcp
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49665]
     Annotation: DHCP Client LRPC Endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49665]
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
     Annotation: DHCPv6 Client LRPC Endpoint
     UUID: a500d4c6-0dd1-4543-bc0c-d5f93486eaf8, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49665]
     UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49665]
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49665]
     Annotation: Event log TCPIP
Port: 49666/tcp
     UUID: 0d3c7f20-1c8d-4654-a1b3-51563b298bda, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49666]
     Annotation: UserMgrCli
     UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49666]
     Annotation: Proxy Manager provider server endpoint
     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49666]
     UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49666]
     Annotation: IP Transition Configuration endpoint
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49666]
     UUID: b18fbab6-56f8-4702-84e0-41053293a869, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49666]
     Annotation: UserMgrCli
     UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49666]
     Annotation: Proxy Manager client server endpoint
     UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49666]
     Annotation: Adh APIs
     UUID: d09bdeb5-6171-4a34-bfe2-06fa82652568, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49666]
Port: 49667/tcp
     UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
     Endpoint: ncacn_ip_tcp:172.16.2.90[49667]
     Annotation: RemoteAccessCheck
     UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49667]
     Named pipe : lsass
     Win32 service or process : Netlogon
     Description : Net Logon service
     UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
     Endpoint: ncacn_ip_tcp:172.16.2.90[49667]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : LSA access
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49667]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
     UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49667]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49667]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:172.16.2.90[49667]
     Annotation: KeyIso
     UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49667]
     Annotation: Impl friendly name
     UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
     Endpoint: ncacn_ip_tcp:172.16.2.90[49667]
     Annotation: MS NT Directory DRS Interface
Port: 49671/tcp
     UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
     Endpoint: ncacn_ip_tcp:172.16.2.90[49671]
     Annotation: RemoteAccessCheck
     UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49671]
     Named pipe : lsass
     Win32 service or process : Netlogon
     Description : Net Logon service
     UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
     Endpoint: ncacn_ip_tcp:172.16.2.90[49671]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : LSA access
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49671]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : SAM access
     UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49671]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49671]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:172.16.2.90[49671]
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
     Annotation: KeyIso
     UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
     Endpoint: ncacn_ip_tcp:172.16.2.90[49671]
     Annotation: MS NT Directory DRS Interface
Port: 49672/tcp
     UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
     Endpoint: ncacn_http:172.16.2.90[49672]
     Annotation: RemoteAccessCheck
     UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
     Endpoint: ncacn_http:172.16.2.90[49672]
     Named pipe : lsass
     Win32 service or process : Netlogon
     Description : Net Logon service
     UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
     Endpoint: ncacn_http:172.16.2.90[49672]
     Named pipe : lsass
     Win32 service or process : lsass.exe
     Description : LSA access
     UUID: 51a227ae-825b-41f2-b4a9-1ac9557a1018, version 1
     Endpoint: ncacn_http:172.16.2.90[49672]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_http:172.16.2.90[49672]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_http:172.16.2.90[49672]
     Annotation: KeyIso
     UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
     Endpoint: ncacn_http:172.16.2.90[49672]
     Annotation: MS NT Directory DRS Interface
Port: 49674/tcp
     UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49674]
     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49674]
     Named pipe : spoolss
     Win32 service or process : spoolsv.exe
     Description : Spooler service
     UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49674]
     UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49674]
     UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49674]
Port: 49677/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
     Endpoint: ncacn_ip_tcp:172.16.2.90[49677]
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
Port: 49691/tcp
     UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5
     Endpoint: ncacn_ip_tcp:172.16.2.90[49691]
     Named pipe : dnsserver
     Win32 service or process : dns.exe
     Description : DNS Server
Port: 49850/tcp
     UUID: 897e2e5f-93f3-4376-9c9c-fd2277495c27, version 1
     Endpoint: ncacn_ip_tcp:172.16.2.90[49850]
     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`

[return to 172.16.2.90]

2.3.3 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: 18516786
Packet 2: 18517867
```

Impact

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

. . . continues on next page . . .

. . . continued from previous page . . .

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
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 172.16.2.90]

2.4 172.16.2.91

Host scan start Tue Dec 5 08:45:59 2023 UTC
Host scan end Tue Dec 5 08:50:16 2023 UTC

Service (Port)	Threat Level
general/tcp	Low
general/icmp	Low

2.4.1 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: 2502659848
Packet 2: 2502660913
```

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
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 172.16.2.91]

2.4.2 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

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

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

Vulnerability Detection Method
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2022-11-18T10:11:40Z`

References
`cve: CVE-1999-0524`
`url: http://www.ietf.org/rfc/rfc0792.txt`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`
`dfn-cert: DFN-CERT-2014-0658`

[return to 172.16.2.91]

2.5 172.16.2.97

Host scan start	Tue Dec 5 08:45:59 2023 UTC
Host scan end	Tue Dec 5 09:02:17 2023 UTC

Service (Port)	Threat Level
general/tcp	Low

. . . (continues) . . .

. . . (continued) . . .

Service (Port)	Threat Level
general/icmp	Low

2.5.1 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: 1213959703
Packet 2: 272683887
```

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
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

. . . continues on next page . . .

. . . continued from previous page . . .

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 172.16.2.97]

2.5.2 Low general/icmp

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

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

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

Vulnerability Detection Method
Details: ICMP Timestamp Reply Information Disclosure
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: 2022-11-18T10:11:40Z

References
cve: CVE-1999-0524
url: http://www.ietf.org/rfc/rfc0792.txt
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658

[return to 172.16.2.97]

This file was automatically generated.