Scan Report

August 7, 2024

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 “Small Network”. The scan started at Tue Aug 6 18:01:33 2024 UTC and ended at Wed Aug 7 04:08:36 2024 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
192.168.67.131 DESKTOP-58VCUC1	0	1	0	0	0
192.168.67.128	0	0	1	0	0
192.168.67.132	0	0	1	0	0
Total: 3	0	1	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 3 results selected by the filtering described above. Before filtering there were 22 results.

2 Results per Host

2.1 192.168.67.131

Host scan start	Tue Aug 6 18:03:49 2024 UTC
Host scan end	Tue Aug 6 18:33:47 2024 UTC

Service (Port)	Threat Level
135/tcp	Medium

2.1.1 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.

. . . continues on next page . . .

. . . continued from previous page . . .

Quality of Detection (QoD): 80%

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: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[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:192.168.67.131[49664]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49664]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:192.168.67.131[49664]
     Annotation: KeyIso
Port: 49665/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49665]
Port: 49666/tcp
     UUID: 3473dd4d-2e88-4006-9cba-22570909dd10, version 5
     Endpoint: ncacn_ip_tcp:192.168.67.131[49666]
     Annotation: WinHttp Auto-Proxy Service
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49666]
     Annotation: DHCP Client LRPC Endpoint
     UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49666]
     Annotation: DHCPv6 Client LRPC Endpoint
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49666]
     Annotation: Event log TCPIP
Port: 49667/tcp
     UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49667]
     UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49667]
     Named pipe : spoolss
     Win32 service or process : spoolsv.exe
     Description : Spooler service
     UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49667]
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
     UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49667]
     UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49667]
Port: 49668/tcp
     UUID: 0497b57d-2e66-424f-a0c6-157cd5d41700, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49668]
     Annotation: AppInfo
     UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49668]
     Annotation: IdSegSrv service
     UUID: 201ef99a-7fa0-444c-9399-19ba84f12a1a, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49668]
     Annotation: AppInfo
     UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49668]
     Annotation: Proxy Manager provider server endpoint
     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49668]
     UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49668]
     Annotation: IP Transition Configuration endpoint
     UUID: 58e604e8-9adb-4d2e-a464-3b0683fb1480, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49668]
     Annotation: AppInfo
     UUID: 5f54ce7d-5b79-4175-8584-cb65313a0e98, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49668]
     Annotation: AppInfo
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49668]
     UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49668]
     Annotation: XactSrv service
     UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49668]
     Annotation: IKE/Authip API
     UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49668]
     Annotation: Proxy Manager client server endpoint
     UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49668]
     Annotation: Adh APIs
     UUID: fd7a0523-dc70-43dd-9b2e-9c5ed48225b1, version 1
     Endpoint: ncacn_ip_tcp:192.168.67.131[49668]
     Annotation: AppInfo
Port: 57614/tcp
     UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
```

. . . continues on next page . . .

... continued from previous page ...

```
     Endpoint: ncacn_ip_tcp:192.168.67.131[57614]
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 192.168.67.131]

2.2 192.168.67.128

Host scan start Tue Aug 6 18:03:49 2024 UTC
Host scan end Wed Aug 7 04:08:26 2024 UTC

Service (Port)	Threat Level
general/icmp	Low

2.2.1 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

... continues on next page ...

. . . continued from previous page . . .

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

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.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2023-05-11T09:09:33Z`

References
```
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[return to 192.168.67.128]

2.3 192.168.67.132

Host scan start Tue Aug 6 18:03:49 2024 UTC
Host scan end Wed Aug 7 04:08:26 2024 UTC

Service (Port)	Threat Level
general/icmp	Low

2.3.1 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

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.

Vulnerability Detection Method
Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2023-05-11T09:09:33Z`

References

```
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[return to 192.168.67.132]

This file was automatically generated.