Scan Report

December 15, 2025

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 "Immediate scan of IP 192.168.2.31". The scan started at Mon Dec 15 22:29:30 2025 UTC and ended at Mon Dec 15 22:37:32 2025 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	Critical	High	Medium	Low	Log	False P.
192.168.2.31	0	0	1	1	0	0
Total: 1	0	0	1	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 2 results selected by the filtering described above. Before filtering there were 12 results.

2 Results per Host

2.1 192.168.2.31

Host scan start	Mon Dec 15 22:30:30 2025 UTC
Host scan end	Mon Dec 15 22:37:29 2025 UTC

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

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 based service enumeration reporting.

Quality of Detection (QoD): 80%

. . . continues on next page . . .

... continued from previous page ...

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:192.168.2.31[49664]
     Annotation: RemoteAccessCheck
     UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
     Endpoint: ncacn_ip_tcp:192.168.2.31[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:192.168.2.31[49664]
     Annotation: Ngc Pop Key Service
     UUID: 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b, version 1
     Endpoint: ncacn_ip_tcp:192.168.2.31[49664]
     Annotation: Ngc Pop Key Service
     UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
     Endpoint: ncacn_ip_tcp:192.168.2.31[49664]
     Annotation: KeyIso
Port: 49665/tcp
     UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
     Endpoint: ncacn_ip_tcp:192.168.2.31[49665]
Port: 49666/tcp
     UUID: 3473dd4d-2e88-4006-9cba-22570909dd10, version 5
     Endpoint: ncacn_ip_tcp:192.168.2.31[49666]
     Annotation: WinHttp Auto-Proxy Service
     UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
     Endpoint: ncacn_ip_tcp:192.168.2.31[49666]
     Annotation: Event log TCPIP
Port: 49667/tcp
     UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1
     Endpoint: ncacn_ip_tcp:192.168.2.31[49667]
     Annotation: IdSegSrv service
     UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1
     Endpoint: ncacn_ip_tcp:192.168.2.31[49667]
     Annotation: Proxy Manager provider server endpoint
     UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
     Endpoint: ncacn_ip_tcp:192.168.2.31[49667]
     UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
     Endpoint: ncacn_ip_tcp:192.168.2.31[49667]
     Annotation: IP Transition Configuration endpoint
     UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
     Endpoint: ncacn_ip_tcp:192.168.2.31[49667]
     UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
```

... continues on next page ...

... continued from previous page ...

```
      Endpoint: ncacn_ip_tcp:192.168.2.31[49667]
      Annotation: XactSrv service
      UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
      Endpoint: ncacn_ip_tcp:192.168.2.31[49667]
      Annotation: IKE/Authip API
      UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1
      Endpoint: ncacn_ip_tcp:192.168.2.31[49667]
      Annotation: Proxy Manager client server endpoint
      UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1
      Endpoint: ncacn_ip_tcp:192.168.2.31[49667]
      Annotation: Adh APIs
      UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
      Endpoint: ncacn_ip_tcp:192.168.2.31[49667]
      Annotation: Impl friendly name
Port: 49668/tcp
      UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
      Endpoint: ncacn_ip_tcp:192.168.2.31[49668]
      UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
      Endpoint: ncacn_ip_tcp:192.168.2.31[49668]
      Named pipe : spoolss
      Win32 service or process : spoolsv.exe
      Description : Spooler service
      UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
      Endpoint: ncacn_ip_tcp:192.168.2.31[49668]
      UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
      Endpoint: ncacn_ip_tcp:192.168.2.31[49668]
      UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
      Endpoint: ncacn_ip_tcp:192.168.2.31[49668]
Port: 49669/tcp
      UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
      Endpoint: ncacn_ip_tcp:192.168.2.31[49669]
      Annotation: RemoteAccessCheck
Port: 49670/tcp
      UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
      Endpoint: ncacn_ip_tcp:192.168.2.31[49670]
Port: 49671/tcp
      UUID: 6b5bdd1e-528c-422c-af8c-a4079be4fe48, version 1
      Endpoint: ncacn_ip_tcp:192.168.2.31[49671]
      Annotation: Remote Fw APIs
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 information to gain more knowledge about the remote host and to conduct further attacks based on it.

... continues on next page ...

... continued from previous page ...

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

Affected Software/OS
All systems exposing / disclosing information via DCE/RPC or MSRPC services.

Vulnerability Insight
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 Method
Reports previously collected (via 'DCE/RPC and MSRPC Services Enumeration' OID: 1.3.6.1.4.1.25623.1.0.108044) DCE/RPC or MSRPC services.
This VT is reporting a severity by default. If the scanned network is e.g. a private LAN / private WAN which contains systems not accessible to the public (access restricted) and it is accepted that the service is disclosing information to this network please set the 'Network type' configuration of the following VT to e.g. 'Private LAN' or 'Private WAN':
Global variable settings (OID: 1.3.6.1.4.1.25623.1.0.12288)
In this case a 'Log' level result is used instead.
Details: `DCE/RPC and MSRPC Services Enumeration Reporting`
OID:1.3.6.1.4.1.25623.1.0.10736
Version used: `2025-11-26T05:40:08Z`

[return to 192.168.2.31]

2.1.2 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

... continues on next page ...

... continued from previous page ...

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: `2025-01-21T05:37:33Z`

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 192.168.2.31]