NetApp Knowledge Base

Does CVE-2022-38023 have any impact to ONTAP 9?

https://kb-stage.netapp.com/on-prem/ontap/da/NAS/NAS-KBs/Does_CVE-2022-38023_have_any_imp…
Updated: Wed, 22 Apr 2026 02:10:15 GMT

Applies to

- ONTAP 9
- FSX
- Cloud Volumes ONTAP (CVO)
- SMB/CIFS
- Netlogon (NTLM Authentication)
- CVE-2022-38023 - Netlogon RPC Elevation of Privilege Vulnerability

Answer

1. ONTAP features configured for domain authentication using NTLMv1 or NTLMv2 e.g. CIFS, Vscan, RBAC, domain tunnel, etc. are affected:

```
::> set advanced
::*> vserver cifs session show -vserver <vserver> -fields auth-
mechanism,address,windows-user
node         vserver   session-id           connection-id
address      auth-mechanism windows-user
------------ --------- -------------------- ------------ ------------
 -------------- ------------
netapp-01a   <vserver> 17134789207261194186 2550496605    10.62.125.
88 NTLMv2          DEMO\user6
netapp-01b   <vserver> 17134789207261194188 2550496606    10.216.29.
42 Kerberos        DEMO\Administrator
2 entries were displayed.
```

Note: If Kerberos authentication attempt fails, NTLM (NTLMv1 or NTLMv2) is default fallback.

2. Impact: All CIFS Domain authentication using NTLM will fail post DC server patch upgrade: CONTAP-80033: NTLM authentication fails due to enforcement of Netlogon RPC sealing
3. Actions as per SU530 are required before June 13, 2023 - "Enforcement by Default" phase when Microsoft's CVE-2022-38023 patches are installed

How do the phases impact ONTAP?

Microsoft Phases	What changed	How did this impact ONTAP 9?	What options do I have?
July 2023 - Enforcement Phase	The Windows updates released on July 11, 2023 will remove the ability to set **RequireSeal:1** **RequireSeal** is forced to be to **2**, contents of the registry value are ignored.	• All NTLM authentication will fail unless you upgrade to a fixed version of CONTAP-80033: NTLM authentication fails due to enforcement of Netlogon RPC sealing • See below: **How ONTAP is impacted once RequireSeal:2 is set**	• Upgrade to a fixed version of CONTAP-80033: NTLM authentication fails due to enforcement of Netlogon RPC sealing • Ensuring clients utilize Kerberos authentication will avoid dependency on Netlogon/NTLM domain authentication

ONTAP impact once RequireSeal:1 is set:

- CONTAP-80033: NTLM authentication fails due to enforcement of Netlogon RPC sealing
- Domain Controller may record following event ID 5838 as **Warning**

ONTAP impact once RequireSeal:2 is set:

- If ONTAP is unpatched, when SVM attempts NTLM authentication, the patched domain controller will return Access Denied causing the request to fail
- EMS Syslog Translator for secd.cifsAuth.problem including the entry:

> FAILURE: Pass-through authentication failed. (NT Status: NT_STATUS_NO_LOGON_SERVERS(0xc000005e))

- EMS also indicate below event to indicate no DC's available.

```
secd.netlogon.noServers: None of the Netlogon servers configured for
Vserver (vs1) are currently accessible via the network.
```

- Domain Controller may record following event ID 5838 as **Error.**

> Log Name: System
> Source: NETLOGON
> Date: 2/22/2023 3:17:28 PM
> Event ID: 5838
> Task Category: None
> Level: Error
> Keywords: Classic
> User: N/A
> Computer: dc1.demo.netapp.local
> Description:
> The Netlogon service encountered a client using RPC signing instead of RPC sealing.
>
> Machine SamAccountName: CIFSSERVERNAME

Additional Information

- We can run below command on Domain Controller to check for event ID 5838.

```
>Get-WinEvent -LogName "System" | Where-Object -Property Id -eq 5838
```

- How to workaround impact seen after applying CVE-2022-38023 on domain controllers after June 13 2023.

- How to manually configure RequireSeal to Compatibility Mode on a Windows domain controller.
- CVE-2022-38023 NetApp context:
  - SU530: [Impact Critical] NTLM authentication fails due to enforcement of Netlogon RPC sealing (Microsoft CVE-2022-38023)
    - NTLM still fails despite setting RequireSeal:1 on DCs for CVE-2022-38023
  - Does CVE-2022-38023 have any impact to Data ONTAP 7-Model
  - December 2022 Samba Vulnerabilities in NetApp Products
- Helpful commands to identify CIFS authentication styles:
  - Client authentication mechanism in use: vserver cifs session show (netapp.com)
  - Auth Style and Domain: vserver cifs show (netapp.com)
  - List discovered DCs: server cifs domain discovered-servers show
- ONTAP user (RBAC) authentication:
  - security login show (netapp.com)
- CIFS / SMB client authentication:
  - How ONTAP handles SMB client authentication (netapp.com)
  - How does an SMB client identify which authentication style to use?
- Kerberos:
  - Check Kerberos settings: vserver cifs security show (netapp.com)
  - ONTAP support for Kerberos
  - ONTAP Requirements for CIFS Kerberos
  - Modify the CIFS server Kerberos security settings
  - What Kerberos Encryption Types are supported with NAS protocols for ONTAP 9