NetApp Knowledge Base

SU530: [Impact Critical] NTLM authentication fails due to enforcement of Netlogon RPC sealing (Microsoft CVE-2022-38023)

https://kb.netapp.com/Support_Bulletins/Customer_Bulletins/SU530

Updated: Mon, 26 Jun 2023 18:22:58 GMT

Summary

[Impact Critical: Cluster data outage]

- To address a vulnerability in the Windows Netlogon RPC code (details in CVE-2022-38023), Microsoft is requiring a new higher level of Netlogon security for Windows Domain Controllers.
- This new level of Netlogon security is being enabled on Microsoft Domain Controllers in a phased approach during regularly scheduled monthly Windows update activity.
- This vulnerability in Windows only applies to domain authentication using NTLM/Netlogon. Authentication via Kerberos or FIPS is not exposed to this vulnerability and is not impacted by the patches being issued by Microsoft to address CVE-2022-38023.
- **Important:** When the Windows updates to address this vulnerability are installed, unless other steps that are documented in this bulletin are taken, NetApp storage systems running versions of ONTAP without a code change to support this higher level of Netlogon RPC security (as tracked under ID 1514175) will experience domain user authentication errors if authenticating via Netlogon, and access to resources shared via CIFS will be impacted.

NetApp's Recommendation

1. Before the June 13, 2023 **"Enforcement by Default"** phase, **either**
   - (preferred) Upgrade all systems running ONTAP to one of the releases in the "Solution" section of this bulletin (or later, as available) **or**
   - Apply the "Compatibility mode" RequireSeal = 1 registry key value to all Windows domain controllers (see the "Workaround" section of this bulletin for more details)
2. Before the July 11, 2023 **"Enforcement"** phase, if not already upgraded, upgrade all systems running ONTAP to one of the releases in the "Solution" section of this bulletin (or later, as available).

Important: After the July 11, 2023 "**Enforcement**" phase there is no workaround for systems running ONTAP 9. ONTAP 9 systems MUST be upgraded to one of the releases in the "Solution" section of this bulletin (or later, as available).

Issue Description

Microsoft is working to a phased implementation schedule for the CVE-2022-38023 change in Windows. As of April 5, 2023, the plan is as follows (based on information taken from KB5021130: How to manage the Netlogon protocol changes related to CVE-2022-38023). As this plan might change further - refer to the Microsoft article for confirmation or updates.

- November 8, 2022 - "Initial deployment" phase

  The initial deployment phase starts with the updates released on November 8, 2022 and continues with later Windows updates until the Enforcement phase. Windows updates on or after November 8, 2022 address security bypass vulnerability of CVE-2022-38023 by enforcing RPC sealing on all Windows clients.

  By default, devices will be set in Compatibility mode. Windows domain controllers will require that Netlogon clients use RPC seal only if they are running Windows, or if they are acting as either domain controllers or as trust accounts.

  There is no impact to ONTAP-based storage virtual machines (SVM) using NTLM/Netlogon authentication during this phase.

- April 11, 2023 - **"Initial enforcement" phase**

  The Windows updates released on or after April 11, 2023 will remove the ability to disable RPC sealing by setting value **0** in the **RequireSeal** registry subkey.

  Under normal circumstances there is no impact to ONTAP-based storage virtual machines (SVM) using

NTLM/Netlogon authentication during this phase (see the FAQ section for some atypical conditions where impact might be experienced).

- June 13, 2023 - **"Enforcement by Default" phase**

  RequireSeal will be moved to "Enforced mode" unless Administrators explicitly configure to be under "Compatibility mode". Vulnerable connections from all clients including third-parties (this includes ONTAP-based SVMs using NTLM/Netlogon authentication) will be denied authentication. See the "Workaround" section below for how to configure "Compatibility mode".

  ONTAP-based SVMs hosted on a system running one of the ONTAP versions in the "Solution" section below (or later as available) will not be impacted during this phase.

- July 11, 2023 **- "Enforcement" phase**

  The Windows updates released on July 11, 2023 will remove the ability to set value **1** in the **RequireSeal** subkey. This enables the final **Enforcement** phase of CVE-2022-38023.

  ONTAP-based SVMs hosted on a system running one of the ONTAP versions in the "Solution" section below (or later as available) will not be impacted.

Note: All domain uses of the Netlogon protocol (NTLMv1 and NTLMv2) are impacted by these changes.

Important: Once the "enforcement" phase is in effect (after July 11, 2023), there is no workaround for ONTAP-based SVMs that authenticate to a Microsoft domain controller using Netlogon/NTLM. All ONTAP systems hosting SVMs that authenticate to a Microsoft domain controller using Netlogon/NTLM MUST upgrade to one of the ONTAP releases in the Solution section of this bulletin (or later, as available) before July 11, 2023, for domain authentication using Netlogon/NTLM to continue. Not doing so will result in an outage to CIFS data services once the July 11, 2023 Windows updates are installed.

Symptom

Once Netlogon RPC Sealing is enabled on a Windows Domain Controller, when an ONTAP-based SVM attempts to pass NTLM authentication information over Netlogon, the Windows Domain Controller will return "Access Denied".

When this happens, ONTAP will report failures in the EMS event log, such as:

> secd.cifsAuth.problem

and

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

The Windows Domain Controller will record event ID: 5838 (example below)

```
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
```

Workaround

Before or during the Microsoft **Enforcement by Default** phase, create the

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\
Parameters\RequireSeal
```

registry key and set the value of `RequireSeal` to `1` on all Windows domain controllers.

This will enable "Compatibility mode". See How to manage Netlogon Protocol changes related to CVE-2022-38023 for more information.

Important: When in the final Microsoft **Enforcement phase** (after July 11, 2023), there is no workaround. The above "Compatibility mode" registry change will not work when in the final **Enforcement phase**, and you will have to be running one of the ONTAP versions listed in the Solution section below (or later, as available) for domain-based Netlogon authentication to work.

(Note that this is **not** the same as the "`RequireSignOrSeal`" registry key that likely already exists in the Windows registry. The "`RequireSignOrSeal`" value has no control over the CVE-2022-38023 patches.)

Solution

Upgrade to a release of ONTAP with the enhancement (tracked in ID 1514175) to support the Microsoft requirement to use Netlogon RPC sealing, as detailed in CVE-2022-38023.

This enhancement is introduced in the following ONTAP releases:

- **9.7P22 (published April 11, 2023)**
  - Cloud Volumes ONTAP version here
- **9.8P18 (published April 19, 2023)**
  - Cloud Volumes ONTAP version here
  - The following 9.8 based Service Updates also include the ID 1514175 enhancement
    - 9.8P19 (published May 27, 2023)
- **9.9.1P15 (published April 7, 2023)**
  - Cloud Volumes ONTAP version here
  - The following 9.9.1 based Service Updates also include the ID 1514175 enhancement
    - 9.9.1P16 (published June 6, 2023)
- **9.10.1P12 (published April 25, 2023)**
  - Cloud Volumes ONTAP version here
  - The following 9.10.1 based Service Updates also include the ID 1514175 enhancement
    - 9.10.1P13 (published June 23, 2023)
- **9.11.1P8 (published April 28, 2023)**
  - Cloud Volumes ONTAP version here
  - The following 9.11.1 based Service Updates also include the ID 1514175 enhancement
    - 9.11.1P9 (published May 17, 2023)
    - 9.11.1P10 (published June 14, 2023)
- 9.12.1P2 (published April 10, 2023)
  - Cloud Volumes ONTAP version here
  - The following 9.12.1 based Service Updates also include the ID 1514175 enhancement
    - 9.12.1P3 (published May 17, 2023)
    - **9.12.1P4 (published June 15, 2023)**
  - **Note that because of other issues seen on systems running ONTAP 9.12.1, the use of 9.12.1P4 (or higher, as available) is strongly recommended for FAS and AFF storage systems running versions of ONTAP 9.12.1**
- 9.13.0P1 (Published April 12, 2023 as a Cloud Volumes ONTAP specific release)
  - The following Cloud Volumes ONTAP 9.13.0 based Service Updates also include the ID 1514175 enhancement
    - 9.13.0P3 (published June 6, 2023)

    - Note that because of a publishing process error specific to the 9.13.0P2 release, 9.13.0P2 does NOT contain the ID 1514175 enhancement.
- 9.13.1RC1 **(published May 4, 2023)**
    - The following 9.13.1 based ONTAP releases also include the ID 1514175 enhancement
        - 9.13.1 (published June 22, 2023)
- ONTAP Select versions of the above ONTAP releases are also available. Visit the ONTAP Select Downloads page for download access.

Note: The releases listed above are all in "Full Support" (as of time of writing) as per the definitions published in the Software Version Support policy page on the NetApp Support Site. Customers running releases of ONTAP 9 that are not in "Full Support" will need to upgrade to one of the above listed releases in order to be able to obtain the enhancement in ONTAP that will allow the continued use of NTLM/Netlogon authentication past Microsoft's final **Enforcement phase**.

Additional Information

Published resources relevant to this bulletin

The following articles published by Microsoft have more information:

- CVE-2022-38023: Netlogon RPC Elevation of Privilege Vulnerability
- KB5021130: How to manage the Netlogon protocol changes related to CVE-2022-38023

The following Resolution Guide published by NetApp has more information that relates to possible impacts from CVE-2022-38023

- How to diagnose and mitigate impact due to CVE-2022-38023 - Resolution Guide

Public Report

- ID 1514175

The following article has information on the various authentication mechanisms available to CIFS/SMB users and how/when they are used.

- How does an SMB client identify which authentication style to use?

Other useful information

To determine which authentication mechanism is in use by CIFS clients, use the following command:

```
      netapp-01::*> 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> 17134789207261194185 2550496604    10.62.125.87
NTLMv1         DEMO\user5
netapp-01a   <vserver> 17134789207261194186 2550496605    10.62.125.88
NTLMv2         DEMO\user6
netapp-01b   <vserver> 17134789207261194188 2550496606    10.216.29.42
Kerberos       DEMO\Administrator

3 entries were displayed.
```

Any entry with an auth-mechanism of NTLMv1 or NTLMv2 is susceptible.

(For more information on this command, see the main ONTAP documentation page for vserver cifs session show.)

Frequently Asked Questions (FAQ)

There's a lot of information in this bulletin. In simple terms what should I do if I think this bulletin might apply to me?

1. Before the June 13, 2023 "**Enforcement by Default**" phase, **either**
   - (preferred) Upgrade all systems running ONTAP to one of the releases in the "Solution" section of this bulletin (or later, as available), **or**
   - Apply the "Compatibility mode" RequireSeal = 1 registry key value to all Windows domain controllers (see the "Workaround" section of this bulletin for more details)
2. Before the July 11, 2023 "**Enforcement**" phase, if not already upgraded, upgrade all systems running ONTAP to one of the releases in the "Solution" section of this bulletin (or later, as available).

Important: After July 11, 2023 there is no workaround for systems running ONTAP 9. ONTAP 9 systems MUST be upgraded to one of the releases in the "Solution" section of this bulletin (or later, as available).

What is "Compatibility mode"?

"Compatibility mode" is when Windows domain controllers patched to address CVE-2022038023 will only require the use of Netlogon RPC Sealing for machines that are running Windows, or if they are acting as either domain controllers or as trust accounts. It is the default mode of operation during the "Initial deployment phase" and the "Initial enforcement phase".

There are 4 stated enforcement phases for CVE-2022-38023 as documented in the Microsoft KB KB5021130: How to manage the Netlogon protocol changes related to CVE-2022-38023.

Before the "Enforcement by Default" (third) phase, setting the **`RequireSeal`** registry key to enable "Compatibility mode" would be a viable workaround until the final "Enforcement" phase is set by the July 11, 2023 Windows update. However, after this final "Enforcement" phase, the only ONTAP solution to address CVE-2022-38023 compatibility is to ensure you are on one of the versions of ONTAP that contain the fix for ID 1514175.

How Do I Set "Compatibility mode" before the June 13, 2023 Update?

You will have to manually add\create\modify the **`RequireSeal`** registry key on your Domain Controllers and set to 1 "Compatibility Mode" per MS KB: KB5021130: How to manage the Netlogon protocol changes related to CVE-2022-38023

This setting will NOT be overridden by the June 13 update.

Note that the key is not created by applying the Microsoft patch - if the key is not present the patch will behave according to the published default behavior. The **`RequireSeal`** registry key, when created, is used to change the behavior from the published default behavior. See KB5021130: How to manage the Netlogon protocol changes related to CVE-2022-38023 for more information.

Also note that this is **not** the same as the "`RequireSignOrSeal`" registry key that likely already exists in the Windows registry. The "`RequireSignOrSeal`" value has no control over the CVE-2022-38023 patches.

Is the use of Kerberos or FIPS with Windows impacted?

No - this change only impacts NTLM/Netlogon authentication with Windows Domain Controllers.

What is the difference between Netlogon RPC signing and sealing?

RPC signing is when the Netlogon protocol uses RPC to sign the messages it sends over the wire. RPC sealing is when the Netlogon protocol both signs and encrypts the messages it sends over the wire.

Is changing to using Kerberos based authentication a workaround for this issue?

While the use of Kerberos for Windows authentication is not exposed to CVE-2022-38023, technically it's not a "workaround", as it results in NTLM/Netlogon authentication not being used any more, and for something to be considered a "workaround" it would allow NTLM/Netlogon authentication to continue to be used. If Kerberos is not already in use in a customer environment, switching to Kerberos will require changes in the customer's authentication environment that require careful planning and implementation.

Note that Domain-Tunnel Kerberos support for Microsoft Active Directory authentication was added to ONTAP through RFE 1351274, and is available in all ONTAP releases as of 9.9.1P8.

What if I am running a version of ONTAP that is earlier than ONTAP 9.7?

Versions of ONTAP earlier than ONTAP 9.7 are no longer in "Full Support" as per the definitions published in the Software Version Support policy page on the NetApp Support Site. Customers running releases of ONTAP that are not in "Full Support" will need to upgrade to one of the above listed releases in order to be able to obtain the enhancement in ONTAP that will allow the continued use of NTLM/ Netlogon authentication past Microsoft's final "Enforcement phase" for CVE-2022-38023.

What if I am running Data ONTAP in 7-Mode?

Customers running with Data ONTAP in 7-Mode are now in "Self Service Support" as per the definitions published in the Software Version Support policy page on the NetApp Support Site. Some guidance for how to address this issue as a result of Microsoft's enforcement of CVE-2022-38023 can be found in Does CVE-2022-38023 have any impact to Data ONTAP 7-Mode.

Do I have to take any other additional action, for example should I enable AES Encryption on my SVMs?

No. In order to address CVE-2022-38023 you do not need to change any settings that are not specifically mentioned in this bulletin.

Is authentication using NTLMv2 also impacted?

Yes. CVE-2022-38023 applies to all uses of the Netlogon protocol, and that includes NTLMv2.

Is it possible to determine what CIFS domain authentication protocol is in use from AutoSupport data sent to NetApp?

While it is possible to use a command to see what authentication protocol is in use (see the "Additional Information" section of this bulletin), that information is not sent via AutoSupport and so NetApp has no visibility of what Windows domain authentication protocol(s) a customer is using.

Do NFS clients (either native or NFS client for Windows) get impacted by this CVE when mapping Unix users to Windows users?

When an NFS client authentication request comes in for an NTFS security style volume, the Unix user will be mapped to a windows user. ONTAP will look that Windows user up via the S4U2self Kerberos extension as opposed to via Netlogon. As such, CVE-2022-38023 should not impact that operation.

The "Solution" section lists a number of ONTAP Service Updates (patch releases) as containing the code change to support CVE-2022-38023. What about releases that come after these?

When a code change is included in a particular Service Update (patch release), all Service Update that follow it will also have that code change. For example, for the ONTAP 9.12.1 release family, the first Service Update that will include the ID 1514175 code change will be 9.12.1P2. That same change will also be in 9.12.1P3. Any Service Update or new release family that follows the versions listed in the "Solution" section will also carry the code change for ID 1514175.

Is there any impact from the Microsoft changes to enforce CVE-2022-38023 to the use of Windows in workgroup mode or to local CIFS users?

Windows operating in workgroup mode, and any authentication that ONTAP might need to do when in a workgroup configuration including local CIFS user authentication (even when SVM is in a domain), does not use Netlogon authentication to a Windows Domain Controller. Authentication is done with local accounts, where ONTAP will use its local SAM database. There should therefore be no impact to workgroup mode or local CIFS user authentication from the Microsoft CVE-2022-38023 changes.

The Microsoft KB article prior to April 20, 2023 said that using a GPO is a valid workaround, but NetApp does not document that - why?

Microsoft had stated the following in KB5021130: "Enforcement mode. All clients are required to use RPC Seal, unless they are added to the "Domain Controller: Allow vulnerable Netlogon secure channel connections" group policy object (GPO)."

NetApp's own testing has found that for supported versions of ONTAP 9, this workaround does not behave as Microsoft have published, and so use of the GPO is not being documented by NetApp as a validated workaround for use with ONTAP 9. This is a limitation in how Windows handles exceptions in the "Domain Controller: Allow vulnerable Netlogon secure channel connections" group policy object (GPO), and it is not possible to work around this limitation for ONTAP 9.

As of April 20, 2023, Micorosft has now removed mention of this workaround, and has added an update note stating "Removed inaccurate reference to "Domain Controller: Allow vulnerable Netlogon secure channel connections" group policy object (GPO) in the "Registry Key settings" section."

I have just applied the April 11 patch from Microsoft and now I am getting authentication issues where previously Netlogon authentication was working. What happened?

The November 8, 2022 version of the CVE-2022-38023 patch from Microsoft didn't behave correctly when the registry key to enforce Netlogon RPC sealing was set ("RequireSeal" = 2). The April 11, 2023 version corrects that. This means that prior to the April 11 update from Microsoft, if "RequireSeal" was set to 2, that no failure events would be logged in the Windows event viewer (event ID:5838 would not be logged, even where a failure and logged event should have been expected).

If you had previously set "RequireSeal" to 2 and have now applied the April 11, 2023 patch from Microsoft to your domain controller(s), your Windows domain controller(s) is(are) now actively enforcing the requirement to use Netlogon RPC sealing, and event ID:5838 will now be logged where appropriate. If you are not running one of the versions of ONTAP that has the change to enable Netlogon RPC sealing (as described in ID 1514175), authentication requests will now be blocked.

If this is the case, you can either set "RequireSeal" to 1 to force compatibility mode (and then plan to upgrade to one of the releases in the "Solution" section of this bulletin some time before July 11, 2023), or you can upgrade ONTAP now to one of the versions listed (as available) and not have to worry about any subsequent changes.

I have just applied the April 11 patch from Microsoft and now I am getting authentication issues where previously Netlogon authentication was working and everything checked indicates that I should be in "Compatibility mode" for Netlogon RPC Sealing. What happened?

NetApp has seen several cases whereby after the April 11 update, even though RequireSeal was set to "1" for "Compatibility mode" (or the key was not present) authentication was still blocked. In these cases, it was found that the Active Directory computer entry for the ONTAP SVM had been somehow modified to identify the ONTAP SVM as a Windows system in the Operating System attribute. When this is done, the MSFT patch treats the ONTAP SVM as if it were a Windows based system, and therefore requires the use of Netlogon RPC Sealing (as per their definition of "Compatibility mode").

If the Active Directory computer entry for the ONTAP SVM identifies the ONTAP SVM as a Windows system, the options are as follows:

- Edit the Active Directory computer entry for the ONTAP SVM to correct the Machine Operating System attributes for the AD object (preferred).
- Delete and recreate the Active Directory computer entry for the ONTAP SVM.
- Upgrade to one of the versions of ONTAP that contain the fix for ID 1514175.

By default, when an Active Directory computer entry is created for an ONTAP SVM, the Machine Operating System attribute will state NetApp Release <version>. It is only when the Machine Operating System attribute has been edited to present the ONTAP SVM as a Windows system that this issue is seen.

For more information on this scenario, see "NTLM still fails despite setting RequireSeal:1 on DCs for CVE-2022-38023"

How is Microsoft releasing the patches to address CVE-2022-38023 in accordance with their published enforcement schedule?

The Microsoft patches that address CVE-2022-38023 are being automatically rolled out during a number of “patch Tuesday” events (November 8, 2022, April 11, 2023, June 13, 2023, July 11, 2023).

Unless the Windows admin has acted to prevent the auto-patching of Windows servers, the relevant patch updates will be automatically installed on those dates. This is something NetApp has NO control over or visibility of, and so NetApp must assume the default behavior of “Windows patches are automatically applied when published” holds true.

If the Windows admin has chosen to defer or stop automatic patching, the statements made in this bulletin regarding Microsoft's implementation phases for CVE-2022-38023 will apply at the time the patches released on the relevant patch Tuesday dates are installed by the Windows admin.

If an ONTAP cluster is only providing SAN and/or NFS services, but is using Domain-Tunnel Authentication for Active Directory (for example, if tunneling authentication requests for FPolicy or Vscan), is there impact from Microsoft CVE-2022-38023?

If the ONTAP system hosting SAN and/or NFS services is running a version of ONTAP earlier than 9.9.1P8 (where NetApp introduced support for domain-tunnel authentication via Kerberos), then domain-tunnel authentication will be via Netlogon and there will be impact. Even if on a release that supports domain-tunnel authentication via Kerberos, if there are other issues that prevent successful Kerberos authentication, the fallback is to use Netlogon unless it has been specifically disabled. As such there could still be impact as a result of the CVE-2022-38023 changes. It is therefore strongly recommended that customers that rely on Domain-Tunnel Authentication for Active Directory upgrade systems running ONTAP to one of the releases in the Solution section of this bulletin.

For more information, see "Does CVE-2022-38023 have impact to Domain-Tunnel Authentication"

If I don't use CIFS but I do use domain user accounts for SSH, API, or GUI login (such as System Manager), is there impact from Microsoft CVE-2022-38023?

If the ONTAP system is running a version of ONTAP earlier than 9.9.1P8 (where NetApp introduced support for domain-tunnel authentication via Kerberos), then domain-tunnel authentication will be via Netlogon and there will be impact. Even if on a release that supports domain-tunnel authentication via Kerberos, if there are other issues that prevent successful Kerberos authentication, the fallback is to use Netlogon unless it has been specifically disabled. As such there could still be impact as a result of the CVE-2022-38023 changes. It is therefore strongly recommended that customers that rely on Domain-Tunnel Authentication for Active Directory upgrade systems running ONTAP to one of the releases in the Solution section of this bulletin.

For more information, see "Does CVE-2022-38023 have impact to Domain-Tunnel Authentication"