Go To Technical Bulletins (/en/user/answers/technical-bulletins.html)

(Alert - NAS 4000 Series, NAS 5000 Series A2023020101r0) HNAS: How to manage the Netlogon protocol changes related to CVE-2022-38023

Type	Alert
Date Posted	02-Feb-2023
Audience	Employee
Products Affected	• NAS 5000 Series • NAS 4000 Series

HNAS: How to manage the Netlogon protocol changes related to CVE-2022-38023

Audience: Employee, Service Partner, Customer
Number: A2023020101r0
Type: Alert

Description

On November 8th, 2022, Microsoft released a security patch to address -

> New netlogin vulnerability:
> Netlogon RPC Elevation of Privilege Vulnerability:
> https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38023 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38023)

This Change requires the use of RPC sealing which is **NOT currently supported on HNAS**.

Microsoft is introducing this change in 3 stages -

> 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 if they are running Windows, or if they are acting as either domain controllers or as trust accounts.
>
> 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 to the RequireSeal.
>
> RequireSeal will be moved to Enforced mode unless Administrators explicitly configure to be under Compatibility mode. Vulnerable connections from all clients including third-parties will be denied authentication.
>
> July 11, 2023 - Enforcement phase
> The Windows updates released on July 11, 2023 will remove the ability to set value 1 to the RequireSeal subkey. This enables the Enforcement phase of CVE-2022-38023.

Registry Key settings

After the Windows updates that are dated on or after November 8, 2022, Windows updates are installed, the following registry key is available for the Netlogon protocol on Windows domain controllers:

RequireSeal

Registry key	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters
Value	RequireSeal
Data type	REG_DWORD
Data	0 – Disabled 1 – Compatibility mode. Windows domain controllers will require that Netlogon clients use RPC Seal if they are running Windows, or if they are acting as either domain controllers or Trust accounts. 2 - 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).
Restart required?	No

Further information can be found in Microsofts KB article -
KB5021130: How to manage the Netlogon protocol changes related to CVE-2022-38023: (https://support.microsoft.com/en-us/topic/kb5021130-how-to-manage-the-netlogon-protocol-changes-related-to-cve-2022-38023-46ea3067-3989-4d40-963c-680fd9e8ee25)

During the initial deployment phase events like these will be logged -

Log Name: System
Source: NETLOGON
Date: 22.11.2022 13:25:10
Event ID: 5840
Task Category: None
Level: Warning
Keywords: Classic
User: N/A
Computer: xxx.yyy.zzz
Description:
The Netlogon service created a secure channel with a client with RC4.

Log Name: System
Source: NETLOGON
Date: 22.11.2022 11:30:08
Event ID: 5838
Task Category: None
Level: Warning
Keywords: Classic
User: N/A
Computer: xxx.yyy.zzz
Description:
The Netlogon service encountered a client using RPC signing instead of RPC sealing.

Affected Products:

- Hitachi NAS Platform 5000 (HNAS 5000)
- Hitachi NAS Platform 4000 (HNAS 4000)
- Hitachi NAS Platform 3080 (HNAS 3080) End of support
- Hitachi NAS Platform 3090 (HNAS 3090) End of Support
- Hitachi Virtual Storage Platform G/Fx00 models (VSP G/Fx00) NAS modules
- Hitachi Virtual Storage Platform Nx00 models (VSP Nx00) NAS modules

Interim Solution

There is a workaround available which can be used allowing more time to upgrade to the enhanced HNAS firmware which supports RPC sealing. The HNAS will need to be added to the "Domain Controller: Allow vulnerable Netlogon secure channel connections" group policy object (GPO).

A step by step procedure for doing this is documented in –
How_to_Configure_Exceptions_for_Netlogon_Functionality
(https://knowledge.hitachivantara.com/Knowledge/Storage/Network_Attached_Storage/Hitachi_NAS_Platform/How_to_Configure_Exceptions_for_Netlogon_Functionality

Permanent Solution

As it will not be possible to upgrade all customers to the 14.6 firmware before the April 11th, 2023 Initial Enforcement Phase It will be necessary to configure Compatibility mode if the Microsoft Security update is going to be applied.

Upgrade to HNAS firmware version 14.6 which is scheduled to release at the beginning of April 2023.

Subscribe here (https://sso.hitachivantara.com/en_us/user/manage-user-subscriptions.html) *to receive Technical Bulletin emails for all your products.*