How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472

▶ *Applies To*

Summary

The Netlogon Remote Protocol (also called MS-NRPC) is an RPC interface that is used exclusively by domain-joined devices. MS-NRPC includes an authentication method and a method of establishing a Netlogon secure channel. These updates enforce the specified Netlogon client behavior to use secure RPC with Netlogon secure channel between member computers and Active Directory (AD) domain controllers (DC).

This security update addresses the vulnerability by enforcing secure RPC when using the Netlogon secure channel in a phased release explained in the Timing of updates to address Netlogon vulnerability CVE-2020-1472 section. To provide AD forest protection, all DCs, must be updated since they will enforce secure RPC with Netlogon secure channel. This includes read-only domain controllers (RODC).

To learn more about the vulnerability, see CVE-2020-1472.

Take Action

To protect your environment and prevent outages, you must do the following:

Note Step 1 of installing updates released August 11, 2020 or later will address security issue in CVE-2020-1472 for Active Directory domains and trusts, as well as Windows devices. To fully mitigate the security issue for third-party devices, you will need to complete all the steps.

Warning Starting February 2021, enforcement mode will be enabled on all Windows Domain Controllers and will block vulnerable connections from non-compliant devices. At that time, you will not be able to disable enforcement mode.

1. UPDATE your Domain Controllers with an update released August 11, 2020 or later.

2. FIND which devices are making vulnerable connections by monitoring event logs.

3. ADDRESS non-compliant devices making vulnerable connections.

4. ENABLE enforcement mode to address CVE-2020-1472 in your environment.

Note If you are using **Windows Server 2008 R2 SP1**, you need an Extended Security Update (ESU) license to successfully install any update that addresses this issue. For more information on the ESU program, please see Lifecycle FAQ - Extended Security Updates.

In this article:

Timing of updates to address Netlogon vulnerability CVE-2020-1472

The updates will be released in two phases: the initial phase for updates released on or after August 11, 2020 and the enforcement phase for updates released on or after February 9, 2021.

August 11, 2020 - Initial Deployment Phase

The initial deployment phase starts with the updates released on August 11, 2020 and continues with later updates until the Enforcement phase. These and later updates make changes to the Netlogon protocol to protect Windows devices by default, logs events for non-compliant device discovery and adds the ability to enable protection for all domain-joined devices with explicit exceptions. This release:

- Enforces secure RPC usage for machine accounts on Windows based devices.

- Enforces secure RPC usage for trust accounts.
- Enforces secure RPC usage for all Windows and non-Windows DCs.
- Includes a new group policy to allow non-compliant device accounts (those that use vulnerable Netlogon secure channel connections). Even when DCs are running in enforcement mode or after the Enforcement phase starts, allowed devices will not be refused connection.
- FullSecureChannelProtection registry key to enable DC enforcement mode for all machine accounts (enforcement phase will update DCs to DC enforcement mode).
- Includes new events when accounts are denied or would be denied in the DC enforcement mode (and will continue in the Enforcement phase). The specific event IDs are explained later in this article.

Mitigation consists of installing the update on all DCs and RODCs, monitoring for new events, and addressing non-compliant devices that are using vulnerable Netlogon secure channel connections. Machine accounts on non-compliant devices can be allowed to use vulnerable Netlogon secure channel connections; however, they should be updated to support secure RPC for Netlogon and the account enforced as soon as possible to remove the risk of attack.

February 9, 2021 - Enforcement Phase

The February 9, 2021 release marks the transition into the enforcement phase. The DCs will now be in enforcement mode regardless of the enforcement mode registry key. This requires all Windows and non-Windows devices to use secure RPC with Netlogon secure channel or explicitly allow the account by adding an exception for the non-compliant device.This release:

- Enforces secure RPC usage for machine accounts on non-Windows based devices unless allowed by "Domain controller: Allow vulnerable Netlogon secure channel connections" group policy.

- Logging of Event ID 5829 will be removed. Since all vulnerable connections are denied, you will now only see event IDs 5827 and 5828 in the System event log.

Deployment Guidelines - deploy updates and enforce compliance

The Initial Deployment Phase will consist of the following steps:

1. Deploying the August 11th updatesto all DCs in the forest.
2. (a) Monitor for warning events and (b) act on each event.
3. (a) Once all warning events have been addressed, full protection can be enabled by deploying DC enforcement mode. (b) All warnings should be resolved before the February 9, 2021 enforcement phase update.

Step 1: UPDATE

Deploy August 11, 2020 updates

Deploy the August 11th updates to all applicable domain controllers (DCs) in the forest, including read-only domain controllers (RODCs). After deploying this update patched DCs will:

- Begin enforcing secure RPC usage for all Windows-based device accounts, trust accounts and all DCs.
- Log event IDs 5827 and 5828 in the System event log, if connections are denied.
- Log event IDs 5830 and 5831 in the System event log, if connections are allowed by "Domain controller: Allow vulnerable Netlogon secure channel connections" group policy.

- Log event ID 5829 in the System event log whenever a vulnerable Netlogon secure channel connection is allowed. These events should be addressed before the DC enforcement mode is configured or before the enforcement phase starts on February 9, 2021.

Step 2a: FIND

Detecting non-compliant devices using event ID 5829

After the August 11, 2020 updates have been applied to DCs, events can be collected in DC event logs to determine which devices in your environment are using vulnerable Netlogon secure channel connections (referred to as non-compliant devices in this article). Monitor patched DCs for event ID 5829 events. The events will include relevant information for identifying the non-compliant devices.

To monitor for events, use available event monitoring software or by using a script to monitor your DCs. For an example script that you can adapt to your environment, see Script to help in monitoring event IDs related to Netlogon updates for CVE-2020-1472

Step 2b: ADDRESS

Addressing event IDs 5827 and 5828

By default, supported versions of Windows that have been fully updated should not be using vulnerable Netlogon secure channel connections. If one of these events is logged in the system event log for a Windows device:

1. Confirm that the device is running a supported versions of Windows.

2. Ensure the device is fully updated.

3. Check to ensure that Domain member: Digitally encrypt or sign secure channel data (always) is set to Enabled.

For non-Windows devices acting as a DC, these events will be logged in the system event log when using vulnerable Netlogon secure channel connections. If one of these events is logged:

- **Recommended** Work with the device manufacturer (OEM) or software vendor to get support for secure RPC with Netlogon secure channel

  a. If the non-compliant DC supports secure RPC with Netlogon secure channel, then enable secure RPC on the DC.

  b. If the non-compliant DC DOES NOT currently support secure RPC, work with the device manufacturer (OEM) or software vendor to get an update that supports secure RPC with Netlogon secure channel.

  c. Retire the non-compliant DC.

- **Vulnerable** If a non-compliant DC cannot support secure RPC with Netlogon secure channel before the DCs are in enforcement mode, add the DC using the "Domain controller: Allow vulnerable Netlogon secure channel connections" group policy described below.

> **Warning** Allowing DCs to use vulnerable connections by the group policy will make the forest vulnerable to attack. The end goal should be to address and remove all accounts from this group policy.

Addressing event 5829

Event ID 5829 is generated when a vulnerable connection is allowed during the initial deployment phase. These connections will be denied when DCs are in enforcement mode. In these events, focus on the machine name, domain and

OS versions identified to determine the non-compliant devices and how they need to be addressed.

The ways to address non-compliant devices:

- **Recommended** Work with the device manufacturer (OEM) or software vendor to get support for secure RPC with Netlogon secure channel:

  a. If the non-compliant device supports secure RPC with Netlogon secure channel, then enable secure RPC on the device.

  b. If the non-compliant device DOES NOT currently support secure RPC with Netlogon secure channel, work with the device manufacturer or software vendor to get an update that allows secure RPC with Netlogon secure channel to be enabled.

  c. Retire the non-compliant device.

- **Vulnerable** If a non-compliant device cannot support secure RPC with Netlogon secure channel before DCs are in enforcement mode, add the device using the "Domain controller: Allow vulnerable Netlogon secure channel connections" group policy described below.

> **Warning** Allowing device accounts to use vulnerable connections by the group policy will put these AD accounts at risk. The end goal should be to address and remove all accounts from this group policy.

Allowing vulnerable connections from 3rd party devices

Use the "Domain controller: Allow vulnerable Netlogon secure channel connections" group policy to add non-compliant accounts. This should only be considered a short-term remedy until non-compliant devices are addressed as described above. **Note** Allowing vulnerable connections from non-compliant devices might have unknown security impact and should be allowed with caution.

1. Created a security group(s) for accounts which will be allowed to use a vulnerable Netlogon secure channel.

2. In Group Policy, go to Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options

3. Search for "Domain controller: Allow vulnerable Netlogon secure channel connections".

4. If the Administrator group or if any group not specifically created for use with this Group Policy is present, remove it.

5. Add a security group specifically made for use with this Group Policy to the security descriptor with the "Allow" permission. **Note** The "Deny" permission behaves the same way as if the account was not added, i.e. the accounts will not be allowed to make vulnerable Netlogon secure channels.

6. Once the security group(s) is added, the group policy must replicate to every DC.

7. Periodically, monitor events 5827, 5828 and 5829 to determine which accounts are using vulnerable secure channel connections.

8. Add those machine accounts to the security group(s) as needed. **Best practice** Use security groups in the group policy and add accounts to the group so that membership is replicated through normal AD replication. This avoids frequent group policy updates and replication delays.

Once all non-compliant devices have been addressed, you can move your DCs to enforcement mode (see next section).

Warning Allowing DCs to use vulnerable connections for trust accounts by the group policy will make the forest vulnerable to attack. Trust Accounts are usually named after the trusted domain, e.g.: The DC in domain-a has a trust with a DC in domain-b. Internally, the DC in domain-a has a trust account named "domain-b$" which represents the trust object for domain-b. If the DC in domain-a wants to expose the forest to risk of attack by allowing vulnerable Netlogon secure channel connections from the domain-b trust account, an admin can use Add-adgroupmember –identity "Name of security group" -members "domain-b$" to add the trust account to the security group.

Step 3a: ENABLE

Moving to enforcement mode in advance of the February 2021 enforcement phase

After all non-compliant devices have been addressed, either by enabling secure RPC or by allowing vulnerable connections with the "Domain controller: Allow vulnerable Netlogon secure channel connections" group policy, set the FullSecureChannelProtection registry key to 1.

Note If you are using the "Domain controller: Allow vulnerable Netlogon secure channel connections" group policy, ensure that the group policy has been replicated and applied to all DCs before setting the FullSecureChannelProtection registry key.

When the FullSecureChannelProtection registry key is deployed, DCs will be in enforcement mode. This setting requires that all devices using Netlogon secure channel either:

- Use secure RPC.
- Are allowed in "Domain controller: Allow vulnerable Netlogon secure channel connections" group policy.

Warning Third party clients that don't support secure RPC with Netlogon secure channel connections will be denied when the DC enforcement mode registry key is deployed which can disrupt production services.

Step 3b: Enforcement Phase

Deploy February 9, 2021 updates

Deploying updates released February 9, 2021 or later will turn on DC enforcement mode. DC enforcement mode is when all Netlogon connections are either required to use secure RPC or the account must have been added to the "Domain controller: Allow vulnerable Netlogon secure channel connections" group policy. At this time, the FullSecureChannelProtection registry key is no longer needed and will no longer be supported.

"Domain controller: Allow vulnerable Netlogon secure channel connections" Group Policy

Best practice is to use security groups in the group policy so that membership is replicated through normal AD replication. This avoids frequent group policy updates and replication delays.

Policy path and setting name	Description
Policy path: **Computer**	This security setting determines whether the domain controller bypasses secure RPC for Netlogon secure

Configuration > Windows Settings > Security Settings > Local Policies > Security Options Setting name: **Domain controller: Allow vulnerable Netlogon secure channel connections** Reboot required? No	channel connections for specified machine accounts. This policy should be applied to all domain controllers in a forest by enabling the policy on the domain controllers OU. When the Create Vulnerable Connections list (allow list) is configured: ▪ Allow: The domain controller will allow the specified group/accounts to use a Netlogon secure channel without secure RPC. ▪ Deny: This setting is the same as the default behavior. The domain controller will require the specified group/accounts to use a Netlogon secure channel with secure RPC. **Warning** Enabling this policy will expose your domain-joined devices and your Active Directory forest, which could put them at to risk. This policy should be used as a temporary measure for third party devices as you deploy updates. Once a third party device is updated to support using secure RPC with Netlogon secure channels, the account should be removed from the Create Vulnerable Connections list. To better understand the risk of configuring accounts to be allowed to use vulnerable Netlogon secure channel connections, please visit https://go.microsoft.com/fwlink/?linkid=2133485. Default: This policy is not configured. No machines or trust accounts are explicitly exempt from secure RPC with Netlogon secure channel connections enforcement. This policy is supported on Windows Server 2008 R2 SP1 and later.

Windows event log errors related to CVE-2020-1472

There are three categories of events:

1. Events logged when a connection is denied because vulnerable Netlogon secure channel connection was attempted:

- 5827 (machine accounts) Error
- 5828 (trust accounts) Error

2. Events logged when a connection is allowed because the account was added to the "Domain controller: Allow vulnerable Netlogon secure channel connections" group policy:

- 5830 (machine accounts) Warning
- 5831 (trust accounts) Warning

3. Events logged when a connection is allowed in the initial release which will be denied in the DC enforcement mode:

- 5829 (machine accounts) Warning

Event ID 5827

Event ID 5827 will be logged when a vulnerable Netlogon secure channel connection from a machine account is denied.

Event log	System

Event source	NETLOGON
Event ID	5827
Level	Error
Event message text	The Netlogon service denied a vulnerable Netlogon secure channel connection from a machine account. Machine SamAccountName: Domain: Account Type: Machine Operating System: Machine Operating System Build: Machine Operating System Service Pack: For more information about why this was denied, please visit https://go.microsoft.com/fwlink/?linkid=2133485.

Event ID 5828

Event ID 5828 will be logged when a vulnerable Netlogon secure channel connection from a trust account is denied.

Event log	System

Event source	NETLOGON
Event ID	5828
Level	Error
Event message text	The Netlogon service denied a vulnerable Netlogon secure channel connection using a trust account. Account Type: Trust Name: Trust Target: Client IP Address: For more information about why this was denied, please visit https://go.microsoft.com/fwlink/?linkid=2133485.

Event ID 5829

Event ID 5829 will only be logged during the Initial Deployment Phase, when a vulnerable Netlogon secure channel connection from a machine account is allowed.

When DC enforcement mode is deployed or once the Enforcement phase starts with the deployment of the February 9, 2021 updates, these connections will be denied and Event ID 5827 will be logged. This is why it is important to monitor for Event 5829 during Initial Deployment Phase and act prior to Enforcement phase to avoid outages.

Event log	System
Event source	NETLOGON
Event ID	5829
Level	Warning
Event message text	The Netlogon service allowed a vulnerable Netlogon secure channel connection. Warning: This connection will be denied once the enforcement phase is released. To better understand the enforcement phase, please visit https://go.microsoft.com/fwlink/?linkid=2133485. Machine SamAccountName: Domain: Account Type: Machine Operating System: Machine Operating System Build: Machine Operating System Service Pack:

Event ID 5830

Event ID 5830 will be logged when a vulnerable Netlogon secure channel machine account connection is allowed by "Domain controller: Allow vulnerable Netlogon secure channel connections" group policy.

Event log	System
Event source	NETLOGON
Event ID	5830
Level	Warning
Event message text	The Netlogon service allowed a vulnerable Netlogon secure channel connection because the machine account is allowed in the "Domain controller: Allow vulnerable Netlogon secure channel connections" group policy. Warning: Using vulnerable Netlogon secure channels will expose the domain-joined devices to attack. To protect your device from attack, remove a machine account from "Domain controller: Allow vulnerable Netlogon secure channel connections" group policy after the third-party Netlogon client has been updated. To better understand the risk of configuring machine accounts to be allowed to use vulnerable Netlogon secure channel connections, please visit https://go.microsoft.com/fwlink/?linkid=2133485. Machine SamAccountName: Domain: Account Type: Machine Operating System: Machine Operating System Build: Machine Operating System Service Pack:

Event ID 5831

Event ID 5831 will be logged when a vulnerable Netlogon secure channel trust account connection is allowed by "Domain controller: Allow vulnerable Netlogon secure channel connections" group policy.

Event log	System
Event source	NETLOGON
Event ID	5831
Level	Warning
Event message text	The Netlogon service allowed a vulnerable Netlogon secure channel connection because the trust account is allowed in the "Domain controller: Allow vulnerable Netlogon secure channel connections" group policy. Warning: Using vulnerable Netlogon secure channels will expose Active Directory forests to attack. To protect your Active Directory forests from attack, all trusts must use secure RPC with Netlogon secure channel. Remove a trust account from "Domain controller: Allow vulnerable Netlogon secure channel connections" group policy after the third-party Netlogon client on the domain controllers have been updated. To better understand the risk of configuring trust accounts to be allowed to use vulnerable Netlogon secure channel connections, please visit https://go.microsoft.com/fwlink/?linkid=2133485. Account Type:

Trust Name:

Trust Target:

Client IP Address:

Registry value for enforcement mode

> Warning Serious problems might occur if you modify the registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall the operating system. Microsoft cannot guarantee that these problems can be solved. Modify the registry at your own risk.

The August 11, 2020 updates introduce the following registry setting to enable enforcement mode early. This will be enabled regardless of the registry setting in the Enforcement Phase starting on February 9, 2021:

Registry subkey	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters
Value	FullSecureChannelProtection
Data type	REG_DWORD

Data	1 – This enables enforcement mode. DCs will deny vulnerable Netlogon secure channel connections unless the account is allowed by the Create Vulnerable Connection list in the "Domain controller: Allow vulnerable Netlogon secure channel connections" group policy. 0 – DCs will allow vulnerable Netlogon secure channel connections from non-Windows devices. This option will be deprecated in the enforcement phase release.
Reboot required?	No

Third-party devices implementing [MS-NRPC]: Netlogon Remote Protocol

All third-party clients or servers must use secure RPC with the Netlogon secure channel. Please contact the device manufacturer (OEM) or software vendors to determine if their software is compatible with the latest Netlogon Remote Protocol.

The protocol updates can be found on the Windows Protocol Documentation site.

Frequently Asked Questions (FAQ)

1. What uses Netlogon secure channel?

2. Can third-party solutions be impacted?

3. Why is my DC denying accounts which have been configured in the "Domain controller: Allow vulnerable Netlogon secure channel connections"group policy?

4. I have an Event ID 5827 for a Windows device. I thought you said Windows is not impacted?

5. Do workstations and endpoint devices need to be updated also?

6. Do non-DC Windows servers or other Windows devices need to be updated with the updates released August 11, 2020 or later before updating DCs?

7. Why isn't Windows Server 2008 SP2 updated to address CVE-2020-1472?

8. Do I need ESU for Windows Server 2008 R2 SP1 to address CVE-2020-1472?

9. How do I ensure that my domain controllers are protected?

10. If I’ve deployed updates to all of my domain controllers, is my enterprise protected from CVE-2020-1472?

11. How do I ensure that my Windows domain-joined device identities are protected?

12. How do I ensure that my third-party domain-joined device identities are protected?

13. What is enforcement mode?

14. What machine accounts should be added to the "Domain controller: Allow vulnerable Netlogon secure channel connections" group policy?

15. What can an attacker do to machine accounts that are on the "Domain controller: Allow vulnerable Netlogon secure channel connections" group policy?

16. Why would I want to add a machine account to the "Domain controller: Allow vulnerable Netlogon secure channel connections" group policy?

17. When would I want to enable enforcement mode?

Glossary

Term	Definition
AD	Active Directory
DC	Domain Controller
Enforcement mode	The registry key that allows you to enable enforcement mode in advance of February 9, 2021.
Enforcement Phase	Phase starting with the February 9, 2021 updates where enforcement mode will be enabled on all Windows Domain Controllers, regardless of the registry setting. DCs will deny vulnerable connections from all non-compliant devices, unless they are added to the "Domain controller: Allow vulnerable Netlogon secure channel connections" group policy.
Initial Deployment Phase	Phase starting with the August 11, 2020 updates and continues with later updates until the Enforcement phase.

machine account	Also referred to as Active Directory Computer or computer object. Please see the MS-NPRC glossary for full definition.
MS-NRPC	Microsoft Netlogon Remote ProtoCol
Non-compliant device	A non-compliant device is one that uses a vulnerable Netlogon secure channel connection.
RODC	read-only domain controllers
Vulnerable connection	A vulnerable connection is a Netlogon secure channel connection that does not use secure RPC.

SUBSCRIBE RSS FEEDS

Need more help?

How can we help you? →

Want more options?

Discover Community

Explore subscription benefits, browse training courses, learn how to secure your device, and more.

Microsoft 365 subscription benefits

Microsoft 365 training

Microsoft security

Accessibility center

Was this information helpful? Yes No

What's new

Surface Pro

Surface Laptop

Surface Laptop Studio 2

Surface Laptop Go 3

Microsoft Copilot

AI in Windows

Explore Microsoft products

Windows 11 apps

Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Microsoft 365 Copilot

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

✓✕ Your Privacy Choices

Consumer Health Privacy

Sitemap Contact Microsoft Privacy Terms of use Trademarks Safety & eco Recycling About our ads