KB5021131: How to manage the Kerberos protocol changes related to CVE-2022-37966

▶ *Applies To*

Change log

Change 1: June 19, 2023:

- Clarified the sentence beginning "To help secure..." in the "Summary" section.
- Added more information to the **Note** in the **DefaultDomainSupportedEncTypes** registry key setting.

In this article

Summary

The Windows updates released on or after November 8, 2022 address security bypass and elevation of privilege vulnerability with Authentication Negotiation by using weak RC4-HMAC negotiation.

This update will set AES as the default encryption type for session keys on accounts that are not marked with a default encryption type already.

To help secure your environment, install Windows updates released on or after November 8, 2022, to all devices, including domain controllers. See Change 1.

To learn more about these vulnerabilities, see CVE-2022-37966.

Discovering Explicitly Set Session Key Encryption Types

You may have explicitly defined encryption types on your user accounts that are vulnerable to CVE-2022-37966. Look for accounts where DES / RC4 is explicitly enabled but not AES using the following Active Directory query:

```
Get-ADObject -Filter "msDS-supportedEncryptionTypes -bor 0x7 -and -not msDS-supportedEncryptionTypes -bor 0x18"
```

Registry Key settings

After installing the Windows updates that are dated on or after November 8, 2022, the following registry key is available for the Kerberos protocol:

DefaultDomainSupportedEncTypes

Registry key	HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\KDC
Value	DefaultDomainSupportedEncTypes
Data type	REG_DWORD
Data value	0x27 (Default)
Restart required?	No

Note If you must change the default Supported Encryption Type for an Active Directory user or computer, manually add, and configure the registry key to set the new Supported Encryption Type. This update does not automatically add the registry key.

Windows domain controllers use this value to determine the supported encryption types on accounts in Active Directory whose **msds-SupportedEncryptionType** value is either empty or not set. A computer that is running a supported version of the Windows operating system automatically sets the **msds-SupportedEncryptionTypes** for that machines account in Active Directory. This is based on the configured value of encryption types that the Kerberos protocol is allowed to use. For more information, see Network security: Configure encryption types allowed for Kerberos.

Users accounts, Group Managed Service accounts, and other accounts in Active Directory do not have the **msds-SupportedEncryptionTypes** value set automatically.

To find Supported Encryption Types you can manually set, please refer to Supported Encryption Types Bit Flags. For more information, see what you should do first to help prepare the environment and prevent Kerberos authentication issues.

The default value **0x27** (DES, RC4, AES Session Keys) was chosen as the minimum change necessary for this security update. We recommend customers set the value to **0x3C** for increased security as this value will allow for both AES-encrypted tickets and AES session keys. If customers have followed our guidance to move to an AES-only environment where RC4 is not used for the Kerberos protocol, we recommend that customers set the value to **0x38**. See Change 1.

Windows events related to CVE-2022-37966

The Kerberos Key Distribution Center lacks strong keys for account

Event Log	System
Event Type	Error
Event Source	Kdcsvc
Event ID	42
Event Text	The Kerberos Key Distribution Center lacks strong keys for account: *accountname*. You must update the password of this account to prevent use of insecure cryptography. See https://go.microsoft.com/fwlink/?linkid=2210019 to learn more.

If you find this error, you likely must reset your krbtgt password before setting KrbtgtFullPacSingature = 3, or installing Windows Updates released on or after July 11, 2023. The update that programmatically enables enforcement mode for CVE-2022-37967 is documented in the following article in the Microsoft Knowledge Base:

KB5020805: How to manage Kerberos protocol changes related to CVE-2022-37967

For more information about how to do this, see the New-KrbtgtKeys.ps1 topic on the GitHub website.

Frequently Asked Questions (FAQ) and Known Issues

- Under what circumstances is my environment vulnerable?
- What should I do first to help prepare my environment and prevent Kerberos authentication issues after installing updates released on or after November 8, 2022 on domain controllers?
- How can I verify that all my devices have a common Kerberos Encryption type?
- I'm having Kerberos authentication issues in my environment after installing updates released on or after November 8, 2022. Do I need to address these issues on Windows client devices or Windows Servers which do not run the Domain Controller role?
- After installing updates released on or after November 8, 2022 on domain controllers, I am experiencing a memory leak with the Local Security Authority Subsystem Service (LSASS.exe). What can I do?
- Why am I having Kerberos authentication failures with non-Windows devices in my environment?

My devices running an unsupported version of Windows are no longer able to access resources in my environment. Also, these devices are unable to be accessed from updated Windows devices in my environment. What can I do?

All my devices have a common Encryption type and are configured to use AES only. Why am I still seeing Kerberos authentication errors after installing the November 8, 2022 update specifically?

I am using an application on my Windows devices which uses a non-Microsoft implementation of Kerberos and I am seeing Kerberos authentication issues. What can I do?

I have msds-SupportedEncryptionTypes set in Active Directory for all accounts configured as non-zero without any Encryption type bits set (least significant 5 bits) but I am having authentication failures after installing updates released on or after November 8, 2022 on domain controllers. What can I do?

Glossary

Advanced Encryption Standard (AES)

Kerberos

Key Distribution Center (KDC)

RC4-HMAC

Session Key

Ticket-granting Ticket

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