Preventing Kerberos change password that use RC4 secret keys

Preventing Kerberos change password that uses RC4 secret keys

This topic for the IT professional explains some limitations in the Kerberos protocol that could lead to a malicious user taking control of a user's account. There is a limitation in the Kerberos Network Authentication Service (V5) standard (RFC 4120), which is well-known within the industry, whereby an attacker can authenticate as a user or change that user's password if the attacker knows the user's secret key.

Possession of a user's password-derived Kerberos secret keys (RC4 and Advanced Encryption Standard [AES] by default) is validated during the Kerberos password change exchange per RFC 4757. The user's plaintext password is never provided to the Key Distribution Center (KDC), and by default, Active Directory domain controllers do not possess a copy of plaintext passwords for accounts. If the domain controller does not support a Kerberos encryption type, that secret key cannot be used to change the password.

In the Windows operating systems designated in the Applies To list at the beginning of this topic, there are three ways to block the ability to change passwords by using Kerberos with RC4 secret keys:

- Configure the user account to include the account option Smart card is required for interactive logon. This limits the user to only signing in with a valid smart card so that RC4 authentication service requests (AS-REQs) are rejected. To set the account options on an account, right-click on the account, the click Properties, and click the Account tab.
- Disable RC4 support for Kerberos on all domain controllers. This requires a minimum of a Windows Server 2008 domain functional level and an environment where all Kerberos clients, application servers, and trust relationships to and from the domain must support AES. Support for AES was introduced in Windows Server 2008 and Windows Vista.

  Note

  There is a known issue with disabling RC4 which can cause the system to restart. See the following hotfixes:

  - Windows Server 2012 R2
  - Windows Server 2012
  - No hotfix is available for earlier versions of Windows Server

- Deploy domains set to Windows Server 2012 R2 domain functional level or higher, and configure users as members of the Protected Users security group. Because this feature disrupts more than just RC4 usage in the Kerberos protocol, see resources in the following See also section.

See Also

- For information about how to prevent the usage of the RC4 encryption type in Windows Server 2012 R2 domains, see Protected Users Security Group.
- For explanations about RFC 4120 and RFC 4757, see IETF Documents.

Additional resources

Events

Windows Server Summit

Apr 29, 9 PM - May 1, 2 AM

Join the ultimate Windows Server virtual event April 29-30 for deep-dive technical sessions and live Q&A with Microsoft engineers.

Sign up now

Training

Module

Secure Windows Server user accounts - Training

Protect your Active Directory environment by securing user accounts to least privilege and placing them in the Protected Users group. Learn how to limit authentication scope and remediate potentially insecure accounts.

Certification

Microsoft Certified: Information Security Administrator Associate(beta) - Certifications

As an Information Security Administrator, you plan and implement information security of sensitive data by using Microsoft Purview and related services. You're responsible for mitigating risks by protecting data inside collaboration environments that are managed by Microsoft 365 from internal and external threats and protecting data used by AI services. You also implement information protection, data loss prevention, retention, insider risk management, and manage information security alerts and activities.