|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Group 1955695160, Grouped object |  | Domain User with Kerberos Pre-Authentication Disabled | | |
| **Findings Categorization** | | | | |
| **Business Impact** | | High | **CVSS v4.0 Score** |  |
| **CVSS Vector** | |  | | |

Technical Description

Kerberos is an authentication protocol used by Active Directory to verify the identity of a user or host. Kerberos performs pre-authentication which takes place during the Authentication Service (AS) exchange and occurs when the client first authenticates to the Key Distribution Center (KDC). This demands that the requestor demonstrates knowledge of the key associated with the account. If the requestor cannot demonstrate this knowledge, the KDC will not issue a Ticket-Granting Ticket (TGT).

If the UF\_DONT\_REQUIRE\_PREAUTH flag is set in the domain users’ userAccountControl attribute, the account does not require Kerberos pre-authentication to logon. An attacker can request a TGT, and session key associated with the TGT, without requiring knowledge of the user’s credentials. Afterwards, the session key can be cracked offline to retrieve the user’s credentials.

Business Impact Description

Kerberos pre-authentication requires users to have knowledge of their credentials in order to retrieve a TGT and its associated session key. If Kerberos pre-authentication is not required, an attacker can request the domain user’s TGT and session key and attempt to crack them offline. Depending on the password strength and complexity of the account, an attacker can potentially retrieve these credentials to authenticate to the domain and further their access in the corporate network.

Affected Users

CENTRAL-05 identified the following users that do not require Kerberos Pre-Authentication:

* Internal\User1
* Internal\User2

Finding Evidence

CENTRAL-05 engineers utilized the tool Impacket-GetNPUsers to perform an LDAP query and identify users with UF\_DONT\_REQUIRE\_PREAUTH set in their userAccountControl attribute.

|  |  |
| --- | --- |
|  | Impacket-GetNPUsers |

/screenshot1

Engineers found 2 users with Kerberos pre-authentication not required.

/screenshot2

Engineers cracked the passwords of both users and authenticated to the domain with both accounts.

Mitigations:

* Enable Kerberos pre-authentication in the identified user accounts:
  + Open Server Manager > Open Active Directory Users and Computers
  + Expand the domain node > Expand the Users Organizational Unit > Select the user
  + Right click > Properties > Go to the Accounts tab > Scroll down > Uncheck the “Do not require Kerberos preauthentication” box
* Enforce a strong password policy to reduce the likelihood of passwords being cracked offline.

References

* [**Impacket GetNPUsers**](https://github.com/fortra/impacket/blob/master/examples/GetNPUsers.py)
* [**Kerberos Pre-Authentication**](https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-kile/4ce3ddc0-aaaa-4a1b-b48b-62a07e906926)
* [**Kerberos RFC 4120**](https://datatracker.ietf.org/doc/html/rfc4120)
* [**User Account Attributes Flags**](https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-samr/10bf6c8e-34af-4cf9-8dff-6b6330922863)

**END OF FINDING BLOCK**