Scope:

Requirements 4.2.5.1, 4.2.5.2, and 4.2.5.3 each address certain risks which may arise when credentials are transmitted over networks in an insecure manner. Common configurations of Active Directory Domain Services may expose AD users’ credentials in this way.

Intent:

Provide a process by which credentials exposed to possible compromise through the use of unsigned, i.e. unencrypted, BINDs or the use of NTLMv1 are identified and become ineligible for Silver assertions.

Risks:

In Active Directory Domain Services environments where the domain controllers have not yet or will not be configured in a way to prevent the use of unsigned LDAP BINDs and Windows network authentication based on either LANMAN or NTLMv1 protocols, user credentials may be transmitted either in the clear or through provably insecure authentication protocols.

The risk is mitigated by an automated audit process which identifies all such users and in cases where the users have been vetted for Silver assertions revokes their eligibility for Silver. This process takes place on a daily basis, so that any potentially compromised credential will be invalidated on average within 12 hours and at a maximum of 24 hours of exposure, which is within the constraints of requirement 4.24.2. The client side cause will then have to be identified and resolved, at which point the user may recertify their credentials using whatever approved process the IdPO has established for such. In the event that the end user recertifies their credentials without resolving the client-side issue or a different issue arises, the credentials will be invalidated by the next failing audit.

Assertion:

For each of requirements 4.2.5.1, 4.2.5.2, and 4.2.5.3, the process of auditing the use of unsigned BINDs and non-NTLMv2 authentication used with the Active Directory Domain Services environment exceeds the requirements in that it assumes that any user’s credentials exposed on the network have been compromised regardless of any other evidence in support or contradiction of that.

Additional Documentation: