ADVISORY: Microsoft Update to Enable LDAP Signing / Channel Binding – 2020H2

Sharing Guideline: PUBLIC (TLP:WHITE)

Executive Summary

LDAP channel binding and LDAP signing provide for secure communications between LDAP clients and servers in an Active Directory Domain. The default configurations for binding and signing are unsafe because they permit LDAP clients to communicate with servers in a manner that opens the door to man-in-the-middle, impersonation, and elevation of privilege attacks. In the second half of 2020, a planned Microsoft security update will change the LDAP channel binding and LDAP signing to more secure configurations [1]. This change may disrupt clients that rely on the unsafe methods.

Recommended Action, between now and the planned 2020 update:

1. Review the sections **AUDITING LDAP Signing** and **AUDITING LDAP Channel Binding** of this Microsoft blog post [2] for steps to enable server auditing and the Windows EventIDs that correspond to LDAP clients that may stop working after the update.
2. Identify and fix OS and application compatibility issues, including but not limited to the use of LDAP non-secure simple binds (LDAP TCP/389 by default) or unsigned SASL (Negotiate, Kerberos, NTLM, or Digest).
3. Consider preemptively enabling LDAP channel binding and signing via registry keys according to Microsoft's guidance [3, 4].

Further Information

This change may especially impact legacy services configured before signing and secure LDAP authentication were more widespread. Services that rely on third-party LDAP frameworks may represent areas to review. This will impact any service that binds via LDAP rather than LDAPS with properly trusted certificates. One specific example could be AD-bound MacOS clients where the output of dsconfigad -show should reflect a "Packet signing" value of **allow** OR **require** and a "Packet encryption" value of **ssl**. This, however, may not be the default behavior and could require rebinding clients.

Third-party PowerShell modules are available for enabling diagnostics / reporting on insecure LDAP binds [5]. These have not been tested or verified by REN-ISAC.

It may be possible to roll back LDAP signing and channel binding after the planned 2020 update by editing the related registry keys [3, 4]; however, doing so may re-open attack vectors such as MITM or relaying.

Additional Resources

1. https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV190023
2. https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/ldap-channel-binding-and-ldap-signing-requirements-march-update/ba-p/921536
3. https://support.microsoft.com/en-us/help/4034879/how-to-add-the-ldapenforcechannelbinding-registry-entry
4. https://support.microsoft.com/en-us/help/935834/how-to-enable-ldap-signing-in-windows-server-2008
5. https://evotec.xyz/four-commands-to-help-you-track-down-insecure-ldap-bindings-before-march-2020/#ut..