Security Advisory Report - OBSO-1911-01

Impact of Microsoft Advisory ADV190023 for Unify Customers (Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing)

Release Date: 2019-11-06 15:08:23
Last Update: 2020-03-27 18:52:21

Summary

LDAP (Lightweight Directory Access Protocol) is used to connect to directory services, e.g. to import user data or connect to a phone book to facilitate dialing.

Microsoft has released **Security Advisory ADV190023.** It announces that Microsoft will change the default settings for LDAP as part of a security update **in March 2020**. Microsoft advises customers to activate the settings that are enforced in 2020 ahead of time and validate the impact on the existing customer environment.

This **Informational Advisory** provides guidance and recommendations for **Unify Customers** about the expected impact of the **Microsoft Security Advisory ADV190023.**

Microsoft intends to release a security update on Windows Update to enable LDAP channel binding and LDAP signing hardening changes and anticipate this update will be available **in March 2020**. The purpose is to enforce security settings when using LDAP in a Microsoft environment in order to prevent that flaws are exploited to gain administrative access to the Windows environment.

Microsoft recommendation:

" ...we strongly advise customers to take the following steps at the earliest opportunity":

- Configure your systems to help make LDAP channel binding and LDAP signing on Active Directory Domain Controllers more secure.
- Find and fix any application compatibility issues in the environment.

Unify recommendation:

Make sure that you are using LDAPS (LDAP over TLS) when connecting to a Microsoft LDAP Servers. Validate your solution environment. Follow the Microsoft instructions given in **Microsoft Advisory ADV190023.** Test the changed configuration settings ahead of time. The subsequent sections provide information on Unify products that have LDAP interfaces and their current status of supporting LDAPS.

Details

Impact on Unify products:

Unify is investigating the impact for Unify products using LDAP to connect to a Microsoft Windows Server.
The following impact is expected:

- LDAP connections using TCP can no longer be established after LDAP channel signing is enforced.
- Customers will have to use LDAPS (LDAP over TLS) to connect to Microsoft LDAP servers.

Latest Update (2020-03-27):

Microsoft has updated the Advisory:
On March 10, 2020, Windows updates will add options for administrators to harden the configurations for LDAP channel binding on Active Directory domain controllers.

The updates add:

- Domain controller: LDAP server channel binding token requirements group policy.
- CBT signing events 3039, 3040, and 3041 with event source Microsoft-Windows-ActiveDirectory_DomainService in the Directory Service event log.

Important: The March 10, 2020 and updates in the foreseeable future will not make changes to LDAP signing or LDAP channel binding policies or their registry equivalent on new or existing domain controllers.

Products affected (LDAPS is not yet supported):
OpenStage/OpenScape Desk Phone IP HFA (planned for V3R0.46.0 in Q2/2020)

Affected Products

Products affected (version LDAPS is supported or higher):

OpenScape 4000 (V7 R2.23 and V8 R0)
OpenScape UC (V7 R1)
OpenScape Contact Center (V9 R2 FP1)

OpenScape Contact Center Extensions (V3 R1)
OpenScape Concierge (V4 R0)
OpenScape Xpressions (V7 R1)
OpenScape Deployment Service (V7 R3)
OpenScape Common Management Portal (V7 R4)
OpenScape Accounting Management (V3 R0.5)
OpenScape Xpert System Manager (V6 R0)
OpenStage/OpenScape Desk Phone IP SIP (V3 R5.6.0)
OpenScape Desk Phone CP SIP (V1 R4.7.0)
OpenScape Desk Phone CP HFA (V1 R2.4.0)
OpenScape Cordless IP (V2 R1)
OpenScape Desktop Client Personal Edition (V7 R1.47.67)
Circuit (since Jan 11th 2020)

Products affected (LDAPS is not yet supported):

OpenStage/OpenScape Desk Phone IP HFA (planned for V3R0.46.0 in Q2/2020)
OpenScape Fault Management (planned for V10R0.07.13 and V11R0.01.01)
OpenScape Business (Active Directory Services integration / planned for V3)
OpenScape Business (UC Suite (LDAP Client) / planned for V3)
OpenScape Business (Integrated LDAP Client for Telephony /no fix planned)
Hipath Cordless IP (no fix planned)
OpenScape Alarm Response Pro (in evaluation)

Products not affected:

All products that are not explicitly listed above do not have an LDAP Interface.

Recommended Actions

Unify recommendation:
Investigate your solution environment in order to evaluate the impact:

- Check whether you are using LDAP within the respected product, the **Affected Products** section provides a list of Unify products that have LDAP interfaces.
- Check whether LDAPS (LDAP over TLS) is enabled to connect to the Microsoft LDAP Sever.
- If LDAPS is not yet implemented plan for the migration ahead of time.
- Follow the Microsoft instructions on how to configure the settings for LDAP Signing and LDAP Channel Binding.
- Test LDAP connections after the migration.
- If you experience issues after the migration report the issues via the established support channels .

If you need Migration Support for the implementation of LDAPS please contact your Unify Partner or your Atos Representative.

References

Additional information available from Microsoft

ADV190023 | Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV190023

2020 LDAP channel binding and LDAP signing requirement for Windows
https://support.microsoft.com/en-us/help/4520412/2020-ldap-channel-binding

Domain controller: LDAP server signing requirements
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/domain-controller-ldap-server-signing-requirements

How to add the LdapEnforceChannelBinding entry
https://support.microsoft.com/en-us/help/4034879/how-to-add-the-ldapenforcechannelbinding-registry-entry

CVE-2017-8563 | Windows Elevation of Privilege Vulnerability
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8563

Identifying Clear Text LDAP binds to your DC’s
https://blogs.technet.microsoft.com/russellt/2016/01/13/identifying-clear-text-ldap-binds-to-your-dcs/ .

Other resources:
https://blog.preempt.com/new-ldap-rdp-relay-vulnerabilities-in-ntlm
https://redmondmag.com/articles/2019/09/11/ldap-fix-for-windows-systems.aspx?m=1
https://dirteam.com/sander/2017/07/13/security-thoughts-vulnerability-in-ntlm-credentials-forwarding-with-ldaps-could-allow-elevation-of-privilege-cve-2017-8563-important/
https://borncity.com/win/2017/08/01/beware-of-microsofts-ldap-server-cve-2017-8563/

Advisory: OBSO-1911-01, status: general release
Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer

OpenScape Baseline Security Office
obso@atos.net

Otto-Hahn-Ring 6
D-81739 München
www.unify.com

respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.
Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG.