PACKETFUSION

Connecting the Dots to the Cloud

March 2020: LDAP Channel Binding and LDAP Signing Requirement Update

Summary

A significant change to Microsoft, related to Active Directory is coming. It will impact the ability to service plain-text authentication requests. We'll help you answer five questions about this change.

1. Does it affect you?

Do you currently use Active Directory integrated (LDAP) authentication on your ShoreTel/Mitel system? If so, this change will impact you. This issue will affect all LDAP users across all Windows Server platforms (even Windows Server 2019).

2. What is it?

Vulnerabilities in the way Active Directory integrated applications (applications which authenticate users with the LDAP protocol, specifically) have been identified that could allow unintentional elevation of privileges within your network. Essentially, credentials are being passed through the network in plain text and are susceptible to being intercepted and tampered with. Microsoft will take action to correct this vulnerability, rendering LDAP dependent applications (like Mitel Connect Director) inaccessible for AD users.

3. What is being done about it?

As relates specifically to your ShoreTel/Mitel solution which is integrated with Active Directory/LDAP, we are working diligently with Mitel on the back-end to develop and test a patch. Once we receive this patch it can be applied in your environment to update the LDAP configuration.

4. Do I need to take action?

At this time, other than running through the process to verify if your other processes that use LDAP for authentication are going to be impacted by this change, no action is required on your part. As soon as we have the above mentioned patch, or other actionable intelligence we will send a notice out and schedule next steps accordingly.

5. What if I have other questions?

If you have any questions, reach out to your Packet Fusion account manager. You can always reach us at sales@packetfusion.com, or 925-701-2000.

Important points on the timeline this year

March 2020: This batch of Windows Updates will introduce some new settings for logging and auditing to Windows Servers to help users identify if they are at risk.

Q4 2020: Microsoft intends to correct the vulnerability in the form of a mandatory security update. That is, Active Directory domain controllers will no longer be able to accept plain-text

Important Note

This change impacts a wide range of other platforms and applications as well. We advise you to review network connected printers, storage, and any other solutions that use LDAP authentication for similar weaknesses.

To find out how deeply you are impacted you can enable auditing for LDAP signing. Here is a great article explaining this process in-depth.