



**BEACON LAB**  
C S I R T

**CYBOLT**  
Security Innovation

# Boletín de Alerta

Boletín Nro.: 2024-69

Fecha de publicación: 16/12/2024

Tema: Vulnerabilidad crítica en ActiveDirectory

Traffic Light Protocol (TLP): White



# Boletín de Alerta



## Producto(s) afectado(s):

Protocolo Ligero de Acceso a Directorios (LDAP) de Windows

- Sistema Operativo Windows Server 2008 y superiores
- Sistema Operativo Windows 10 y superiores

## Descripción

Recientemente se ha publicado una vulnerabilidad que afecta al protocolo LDAP, nombrado como CVE-2024-49112, la cual es una falla crítica de ejecución remota de código (RCE) con una puntuación CVSS de 9.8 con riesgo crítico. Afecta al protocolo Protocolo Ligero de Acceso a Directorios (Lightweight Directory Access Protocol - LDAP) de Windows, utilizado ampliamente para la autenticación de servicios de directorio en redes corporativas.

El equipo de Microsoft ha informado que un atacante no autenticado dentro de la red podría aprovechar esta vulnerabilidad enviando un conjunto de llamadas LDAP especialmente diseñado. Esto permitiría ejecutar código arbitrario dentro del contexto del servicio LDAP, comprometiendo gravemente el servidor Active Directory.

## Mitigación

Configurar los servidores de Active Directory para no aceptar llamadas a procedimientos remotos (RPC) provenientes de redes no confiables.

## Solución

Actualmente el proveedor ha publicado una serie de actualización o parche de seguridad para solucionar esta vulnerabilidad, puede encontrar información al respecto en el siguiente enlace:

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49112>

Enlaces de las actualizaciones:

- Windows Server 2019 y Windows 10:  
<https://catalog.update.microsoft.com/Search.aspx?q=KB5048661>
- Windows Server 2012 R2:  
<https://catalog.update.microsoft.com/Search.aspx?q=KB5048735>
- Windows Server 2008, parche de seguridad:  
<https://catalog.update.microsoft.com/Search.aspx?q=KB5048744>

### **Información adicional:**

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49112>
- <https://thehackernews.com/2024/12/microsoft-fixes-72-flaws-including.html>



**BEACON LAB**  
C S I R T

**CYBOLT**   
Security Innovation

[info@beaconlab.mx](mailto:info@beaconlab.mx)

[beaconlab.mx](http://beaconlab.mx)

[contact@cybolt.com](mailto:contact@cybolt.com)

[cybolt.com](http://cybolt.com)

