Nro. Alerta:	AL-2025-001	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	13-ene-2025	(CVE-2024-49113) Vulnerabilidad en LDAP de Windows permite ataques DoS	Pág.: **1** of **4**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Nivel de riesgo: Alta

II. ALERTA

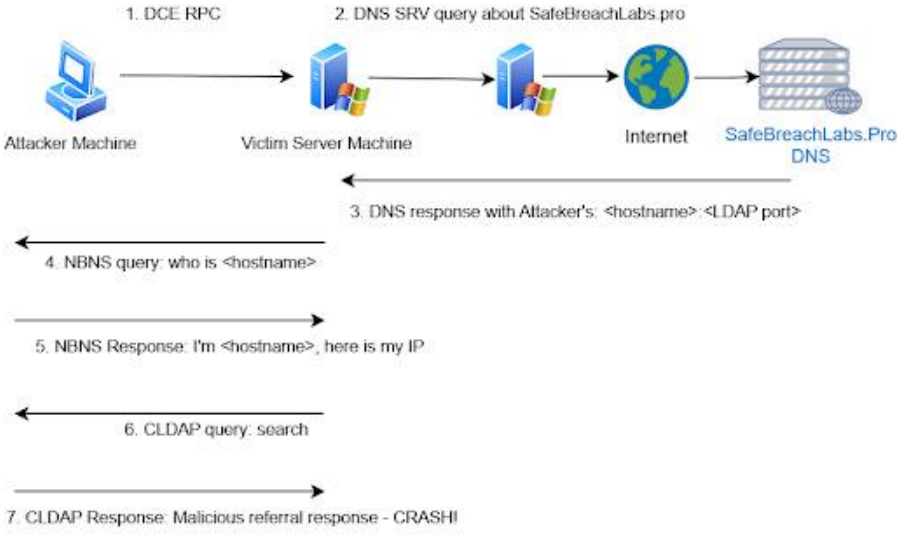

Figura1: *Vulnerabilidad de denegación de servicio del Protocolo LDAP de Windows.*

Investigadores han confirmado la existencia de un exploit bajo la técnica Prueba de Concepto (PoC - técnica de ciberseguridad que se utiliza para demostrar la vulnerabilidad de un sistema) para la vulnerabilidad CVE-2024-49113, también conocida como LDAP Nightmare. El atacante logra explotar esta falla para poder bloquear servidores que no estén parcheados e inclusive ejecutar código malicioso con privilegios elevados y también mediante un exploit se realiza un DoS (Ataque de denegación de servicio) en cualquier servidor Windows (incluyendo controladores de dominio) mandando peticiones LDAP maliciosas.

III. INTRODUCCIÓN

El protocolo LDAP, es un conjunto de protocolos de licencia abierta que son utilizados para acceder a información que esta almacenada de forma centralizada en una red y este se utiliza a nivel de aplicación para acceder a los servicios de directorio remoto.

Microsoft revelo que es una vulnerabilidad crítica que afecta al protocolo LDAP, esta falla de seguridad permite la ejecución de RCE (ejecución remota de código) y es usada por

un atacante no autenticado para comprometer servidores y estaciones de trabajo. El problema viene de un desbordamiento de enteros en el código (que en términos de ciberseguridad es un vulnerabilidad que se produce cuando un programa intenta crear un valor numérico que supera el espacio de memoria asignado para ese tipo de datos) relacionado con el servicio LDAP.

Un atacante, sin necesidad de autenticarse, puede aprovechar esto enviando llamadas RPC (llamada a procedimiento remoto) manipuladas que disparan consultas LDAP maliciosas. Si el ataque tiene éxito, puede hacer que el servidor colapse o usar esa brecha como puerta de entrada para ejecutar código malicioso.

IV. VECTOR DE ATAQUE

CVE-2024-49113 LDAPNightmare Tipo AV:N – Red

El proceso que realiza:

1. El atacante es él envió de una solicitud DCE/RPC (Distributed Computing Environment/Remote Procedure Call) a la máquina del servidor de la víctima.
2. Se activa la víctima para que envíe una consulta DNS SRV sobre el dominio del usuario.
3. El servidor DNS del atacante responde con el nombre de host de la máquina del atacante y el puerto LDAP.
4. La víctima envía una solicitud NBNS (servicio de nombres NetBIOS) de difusión para encontrar la dirección IP del nombre de host recibido (del atacante).
5. El atacante envía una respuesta NBNS con su dirección IP.
6. La víctima se convierte en un cliente LDAP y envía una solicitud CLDAP a la máquina del atacante.
7. El atacante envía un paquete de respuesta de referencia CLDAP con un valor específico que hace que LSASS se bloquee y fuerce el reinicio del servidor de la víctima.

V. IMPACTO

CVE-2024-49113 es un defecto de desbordamiento de enteros en wldap32.dll, una biblioteca que implementa la lógica del cliente LDAP y que su código PoC (Prueba de concepto) no funciona en servidores parcheados.

- Windows Server 2012 R2 (Server Core installation).
- Windows Server 2019 - x64.
- Windows Server 2012 R2.

- Windows Server 2012 (Server Core installation).
- Windows Server 2012.
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation).
- Windows Server 2008 R2 for x64-based Systems Service Pack 1.
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation).
- Windows Server 2008 for x64-based Systems Service Pack 2.
- Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation).
- Windows Server 2008 for 32-bit Systems Service Pack 2.
- Windows Server 2016 (Server Core installation).
- Windows Server 2016.
- Windows 10 Version 1607 for x64-based Systems/32-bit Systems.
- Windows 10 for x64-based Systems/32-bit Systems.
- Windows Server 2025.
- Windows 11 Version 24H2 for x64-based Systems/ARM64-based Systems.
- Windows Server 2022, 23H2 Edition (Server Core installation).
- Windows 11 Version 23H2 for x64-based Systems/ARM64-based Systems.
- Windows Server 2025 (Server Core installation).
- Windows 10 Version 22H2 for 32-bit Systems/ARM64-based Systems/x64-based Systems.
- Windows 11 Version 22H2 for x64-based Systems/ARM64-based Systems.
- Windows 10 Version 21H2 for x64-based Systems/ARM64-based Systems/ 32-bit Systems.
- Windows Server 2022 (Server Core installation).

VI. RECOMENDACIONES:

Las organizaciones deben mantener actualizadas las aplicaciones, aplicando los parches publicados por los fabricantes. Dada la naturaleza crítica de los controladores de dominio y el potencial movimiento lateral dentro de la red de una organización, es esencial abordar este tipo de vulnerabilidades lo antes posible.

Soluciones alternativas recomendadas por Microsoft:

- Asegúrese de que los controladores de dominio estén configurados para no acceder a Internet (nota: es probable que esto no sea factible para la mayoría de las organizaciones).

- Asegúrese de que los controladores de dominio estén configurados para no permitir la RPC entrante desde redes que no sean de confianza.
- Limita el acceso a LDAP solo dentro de tu red.
- Implementa firewalls y monitorea actividad sospechosa.
- Configura firewalls y reglas para bloquear tráfico DCE/RPC, NBNS y CLDAP desde fuentes no confiables.
- Utiliza herramientas SIEM para detectar patrones de ataque en los protocolos mencionados.
- Restringir conexiones RPC y LDAP: Configure los controladores de dominio para bloquear tráfico no confiable desde redes externas.
- Aislar los sistemas críticos: Segmente su red para minimizar el impacto de posibles ataques.
- Revisar las reglas de firewall: Asegúrese de que solo se permita el tráfico necesario hacia los servicios LDAP y RPC.

VII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VIII. REFERENCIAS:

https://www.cve.org/CVERecord?id=CVE-2024-49113

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

https://www.cvedetails.com/cve/CVE-2024-49113/

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49113

https://socprime.com/blog/cve-2024-49112-exploitation-attempts-detection/