Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

VULNERABILIDAD CRÍTICA DE LDAP EN WINDOWS – CVE-2024-49112

13 / 12 / 2024

CONTENIDO

INTRODUCCIÓN

Microsoft ha informado recientemente de una vulnerabilidad crítica que afecta al servicio LDAP en diversas versiones de Windows, conocida como CVE-2024-49112. Esta falla permite que atacantes remotos ejecuten código malicioso sin necesidad de autenticación, representando un riesgo significativo para los sistemas empresariales. Si su organización utiliza Windows, es fundamental comprender el alcance de esta amenaza y actuar de inmediato para proteger sus datos y garantizar la continuidad operativa.

RANSOMWARE TRIGONA DESENCADENA ALARMAS DE CIBERSEGURIDAD EN LA REGIÓN

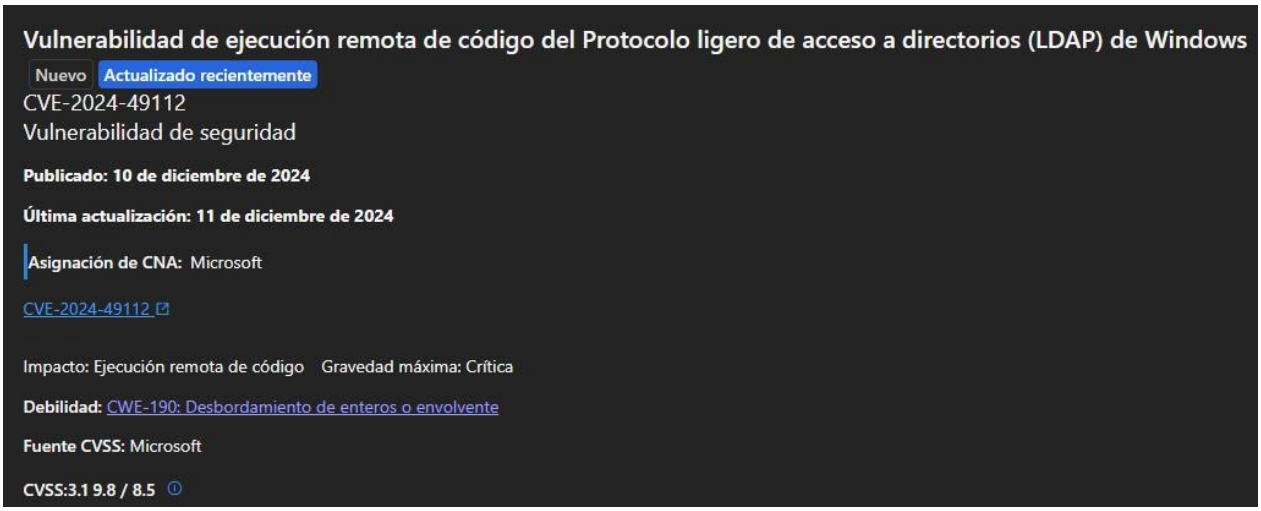
A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_12_13_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	13/12/2024
Es día cero (0 day):	No

Resumen

Microsoft ha revelado recientemente una vulnerabilidad crítica que afecta al Protocolo Ligero de Acceso a Directorios (LDAP) en diversas versiones de Windows. Identificada como CVE-2024-49112, esta falla de seguridad permite la ejecución remota de código (RCE) y podría ser utilizada por atacantes no autenticados para comprometer servidores y estaciones de trabajo.

¿Qué es CVE-2024-49112?



La vulnerabilidad CVE-2024-49112 aprovecha un desbordamiento de enteros (CWE-190) en el manejo de solicitudes RPC por parte del servicio LDAP. Esto podría permitir que un atacante remoto ejecute código arbitrario en el sistema afectado, comprometiendo la confidencialidad, integridad y disponibilidad de los datos.

Impacto técnico

- Gravedad: Crítica (CVSS: 9.8)
- Vector de ataque: Red
- Privilegios requeridos: Ninguno
- Interacción con el usuario: Ninguna

Sistemas afectados

Esta vulnerabilidad impacta tanto a servidores como a clientes de Windows, incluyendo:

- Windows Server: Desde 2008 hasta 2025
- Windows 10: Versiones 1607 a 22H2
- Windows 11: Versiones 22H2 a 24H2

Para consultar la lista completa de versiones, le recomendamos visitar el boletín oficial de Microsoft.

¿Cómo podrían atacarle?

Un atacante podría explotar esta vulnerabilidad de dos maneras principales:

1. En servidores LDAP: Enviando solicitudes RPC maliciosas para provocar búsquedas de controladores de dominio en dominios controlados por el atacante.

2. En clientes LDAP: Convenciendo a la víctima para conectarse a un servidor LDAP malicioso, lo que permitiría la ejecución de código remoto en el contexto del cliente.

En ambos casos, el acceso no autorizado a sus sistemas podría resultar en robo de datos, interrupción de servicios o incluso ransomware.

¿Qué puede hacer para protegerse?

1. Aplica los parches oficiales de Microsoft

La medida más efectiva es instalar las actualizaciones de seguridad lanzadas por Microsoft el 10 de diciembre de 2024. Por ejemplo:

- Para Windows Server 2025, aplique los paquetes 5048667 y 5048794.
- Para Windows 10 versión 22H2, utilice el parche 5048652.

Las actualizaciones están disponibles a través de Windows Update o el Catálogo de Microsoft Update.

2. Implemente mitigaciones provisionales

Si no puede aplicar los parches de inmediato, considere las siguientes acciones:

- 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.

3. Fortalezca su monitoreo y respuesta

- Utilice herramientas de detección de intrusos (IDS/IPS) para identificar patrones de tráfico anómalos hacia servicios LDAP.
- Capacite a su equipo de TI para responder rápidamente a señales de explotación.

Recomendaciones finales

La vulnerabilidad CVE-2024-49112 subraya la importancia de mantener una estrategia sólida de ciberseguridad. Estas son nuestras recomendaciones clave:

- Actualice sus sistemas regularmente.
- Implemente políticas de acceso mínimo (Zero Trust).
- Realice auditorías de seguridad periódicas.

No subestime el impacto potencial de esta vulnerabilidad. Tome medidas hoy para proteger sus sistemas y garantizar la continuidad de su negocio.

Si necesita ayuda para implementar estas medidas, no dude en ponerse en contacto con nosotros. ¡Estamos aquí para ayudarle a mantener su empresa segura!

NOTICIA COMPLETA

https://devel.group/blog/vulnerabilidad-critica-de-ldap-en-windows-cve-2024-49112/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente