# Boletín de alerta

**Boletín Nro.:** 58
**Fecha de publicación:** 03/06/2026
**Tema:** Alerta 2026-58 Vulnerabilidad Crítica en Windows Netlogon
**Traffic Light Protocol (TLP):** White

## Producto(s) afectado(s):

La vulnerabilidad afecta a servidores Windows que operan como Controladores de Dominio mediante el servicio Windows Netlogon.

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

## Descripción

Recientemente, Microsoft reveló la vulnerabilidad CVE-2026-41089, descubierta por su equipo interno Windows Attack Research & Protection (WARP). La falla afecta a Windows Netlogon, un componente crítico responsable de la autenticación y administración de relaciones de confianza dentro de entornos de Active Directory. La vulnerabilidad recibió una puntuación CVSS 9.8 (Crítica) y permite a un atacante remoto no autenticado ejecutar código arbitrario sobre un controlador de dominio mediante solicitudes especialmente diseñadas enviadas a través de la red.

Técnicamente, la vulnerabilidad corresponde a un desbordamiento de búfer basado en pila (CWE-121) dentro del servicio Netlogon. Un atacante puede explotar la falla enviando paquetes manipulados que provocan corrupción de memoria en el proceso responsable de manejar las solicitudes de autenticación del dominio. Debido a que Netlogon opera con altos privilegios y forma parte fundamental de Active Directory, una explotación exitosa podría permitir la ejecución de código con privilegios de SYSTEM sobre el controlador de dominio comprometido.

El impacto es especialmente grave porque la explotación no requiere autenticación previa ni interacción del usuario. En entornos empresariales, un atacante con acceso a la red interna podría utilizar esta vulnerabilidad para comprometer la infraestructura de identidad, expandir privilegios, desplegar malware o incluso tomar control completo del bosque de Active Directory.

Inicialmente Microsoft catalogó la vulnerabilidad como de explotación menos probable; sin embargo, el Centre for Cybersecurity Belgium (CCB) confirmó posteriormente que CVE-2026-41089 está siendo explotada activamente en la naturaleza, elevando significativamente su criticidad y urgencia de remediación.

## Solución:

Microsoft publicó actualizaciones de seguridad para corregir la vulnerabilidad durante el ciclo de actualizaciones de mayo de 2026. Se recomienda aplicar los parches de forma prioritaria en todos los controladores de dominio de la organización durante la misma ventana de mantenimiento para evitar escenarios donde existan entornos parcialmente actualizados que continúen siendo vulnerables.

En el siguiente enlace se encuentra el parche oficial de Microsoft: **https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41089**

Como medida adicional de mitigación, se recomienda restringir el tráfico hacia los controladores de dominio únicamente a los sistemas que realmente requieran acceso a los servicios de autenticación, implementar segmentación de red y revisar la exposición de servicios Netlogon desde segmentos de usuario o redes VPN.

Los equipos de seguridad también deberían monitorear indicadores de posible explotación, incluyendo:

- Reinicios inesperados o fallas del servicio Netlogon.
- Tráfico anómalo dirigido a controladores de dominio.
- Errores de autenticación o fallas de confianza entre dominios.
- Actividad sospechosa en LSASS y procesos relacionados con autenticación.
- Creación de cuentas privilegiadas o modificaciones inesperadas en Active Directory.

## Información adicional:

- **https://nvd.nist.gov/vuln/detail/cve-2026-41089**
- **https://www.helpnetsecurity.com/2026/06/01/windows-netlogon-rce-exploited-cve-2026-41089/**
- **https://www.securityweek.com/critical-windows-netlogon-vulnerability-in-attackers-crosshairs**