Boletín de alerta

Boletín Nro.: 43
Fecha de publicación: 23/04/2026
Tema: Alerta 2026-43 Vulnerabilidad crítica de RCE en Microsoft Windows Active Directory
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Producto	Versiones afectadas
Microsoft Windows Server 2012 R2	Todas las ediciones, incluyendo Server Core.
Microsoft Windows Server 2016	Ediciones estándar y datacenter, incl. Server Core.
Microsoft Windows Server 2019	Todas las ediciones, incl. Server Core.
Microsoft Windows Server 2022	Todas las ediciones, incl. 23H2 y Server Core.
Microsoft Windows Server 2025	Todas las ediciones, incl. Server Core.

Descripción

Se ha identificado la vulnerabilidad crítica CVE-2026-33826 en Microsoft Windows Active Directory, que afecta a múltiples versiones de Windows Server 2012 R2, 2016, 2019, 2022 y 2025, incluyendo instalaciones Server Core. Esta falla de ejecución remota de código (RCE), causada por una validación insuficiente al manejar paquetes, permite a un atacante remoto ejecutar código arbitrario en modo kernel enviando paquetes especialmente manipulados al controlador de dominio. La explotación exitosa podría dar como resultado el compromiso completo del servidor de Active Directory y, por extensión, del dominio asociado.

CVE-2026-33826 es una vulnerabilidad de ejecución remota de código (RCE) en el componente de Active Directory de Microsoft Windows, originada por una validación insuficiente de paquetes, que puede explotarse de forma remota siempre que el atacante pueda enviar paquetes maliciosos al servicio afectado en el controlador de dominio (habitualmente accesible desde redes internas y, potencialmente, desde Internet si se expone de forma indebida); dado que la información pública disponible no especifica claramente si se requiere autenticación o un rol concreto, se recomienda asumir el peor escenario (explotación posible sin autenticación) hasta que Microsoft indique lo contrario, ya que una explotación exitosa permite la ejecución de código arbitrario en el sistema con privilegios de kernel, lo que conlleva el compromiso potencial total del sistema operativo, el despliegue de malware, la desactivación de defensas, el robo o manipulación de credenciales y un movimiento lateral masivo dentro del dominio.

Active Directory es el servicio central de directorio y autenticación en entornos Windows empresariales, usado para la gestión de identidades, políticas de grupo, autenticación de usuarios y servicios críticos (aplicaciones corporativas, acceso a recursos de red, VPN, etc.). Un RCE en el contexto del kernel de un controlador de dominio permite a un atacante tomar control total del servidor, modificar objetos de directorio, crear cuentas privilegiadas, distribuir malware mediante GPO, desactivar defensas y manipular o robar credenciales a gran escala.

Solución

La medida principal es aplicar de forma inmediata los parches de seguridad publicados por Microsoft para CVE-2026-33826 en todos los servidores Windows que actúen como controladores de dominio, priorizando primero aquellos que estén expuestos a redes menos confiables (DMZ, entornos híbridos, segmentos con acceso de terceros) y, a continuación, el resto de controladores. Se recomienda asegurar que todos los servidores Windows Server 2012 R2, 2016, 2019, 2022 y 2025, incluyendo instalaciones Server Core, se actualicen a la última actualización acumulativa mensual que incluya la corrección de este CVE, siguiendo la guía oficial de MSRC.

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33826

Información adicional

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33826
- https://www.fortiguard.com/encyclopedia/ips/60685
- https://www.fortiguard.com/services/ips
- https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-fortinet-products-could-allow-for-arbitrary-code-execution_2026-04-13