Boletín de alerta

Boletín Nro.:
Fecha de publicación: 27/07/2026
Tema: Alerta 2026-77 Vulnerabilidad Crítica en AD CS con PoC Pública
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025
- Windows Server (Server Core)
- Windows 10 versión 1607
- Windows 10 versión 1809
- Entornos que utilicen Active Directory Certificate Services (AD CS) con una Enterprise CA.

Descripción

Se ha divulgado una vulnerabilidad crítica identificada como **CVE-2026-54121 (CVSS 8.8)**, conocida como **Certighost**, que afecta a **Active Directory Certificate Services (AD CS)**. La falla permite que un usuario autenticado con privilegios mínimos obtenga un certificado válido para suplantar la identidad de un **Controlador de Dominio (Domain Controller)**. Una vez autenticado como dicho controlador mediante **PKINIT**, el atacante puede ejecutar un ataque **DCSync** para extraer el secreto **KRBTGT**, comprometiendo por completo el dominio de Active Directory. Aunque Microsoft indicó inicialmente que la explotación era poco probable, actualmente existe una **prueba de concepto (PoC) pública y funcional**, lo que incrementa significativamente el riesgo para las organizaciones que aún no han aplicado las actualizaciones de seguridad.

Solución:

Se recomienda implementar las siguientes acciones de forma inmediata:

- Aplicar las **actualizaciones de seguridad de Microsoft publicadas el 14 de julio de 2026** en todos los servidores que ejecuten **Active Directory Certificate Services (AD CS)**.

- Si no es posible aplicar el parche de inmediato, Microsoft y los investigadores recomiendan, únicamente como medida temporal y tras validarla en un entorno controlado, deshabilitar la funcionalidad de chase ejecutando:

certutil -setreg policy\EditFlags -EDITF_ENABLECHASECLIENTDC

Restart-Service CertSvc -Force

Importante: Esta mitigación puede afectar los procesos legítimos de emisión de certificados y no sustituye la instalación de las actualizaciones de seguridad.

Información adicional:

- **Certighost Exploit Lets Low-Privileged Active Directory Users Impersonate a Domain Controller**
- **Known Exploited Vulnerabilities Catalog | CISA**
- **CVE-2026-54121 – Security Update Guide – Microsoft – Active Directory Certificate Services Elevation of Privilege Vulnerability**