Nro. Alerta:	AL-2026-007	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	18-feb-2025	Vulnerabilidad 0-Day CVE-2026-21533 en Windows RDS (Elevación de Privilegios)	Pág.: **1** of **3**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad crítica – 0-Day en sistemas Windows
Tipo de Incidente: Explotación de vulnerabilidad local en Windows Remote Desktop Services (RDS)
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Vulnerabilidad 0-Day CVE-2026-21533 en Windows RDS (Elevación de Privilegios)- Figura referencial

Microsoft anuncia parche para una Vulnerabilidad 0-day denominada CVE-2026-21533 en Windows Remote Desktop Services (RDS), la cual permite a un atacante autorizado elevar los privilegios localmente, esta falla se deriva del concepto CWE-269 Gestión de privilegios inapropiada.

III. INTRODUCCIÓN

El proveedor de ciberseguridad CrowdStrike reporto a Microsoft sobre la vulnerabilidad CVE-2026-21533, una vulnerabilidad de elevación de privilegios local, para ello un atacante necesita un acceso local inicial con bajos privilegios, es decir ya debe haber obtenido acceso al host vulnerable ya sea mediante un archivo malicioso, otra vulnerabilidad en ejecución remoto de código (RCE) o por movimiento lateral de otro sistema comprometido.

Una vez dentro del host, el atacante realiza la elevación de privilegios al nivel más alto del sistema, SYSTEM (que está por encima del nivel ADMIN), incluso con este nivel de acceso el atacante puede deshabilitar las herramientas de seguridad, esparcir malware, acceder a credenciales, agregar usuarios, eludir defensas, generar backdoors.

IV. VECTOR DE ATAQUE

CrowdStrike reporta un exploit que modifica una clave de configuración de servicio si bien CrowdStrike y Microsoft no informan el nombre exacto del servicio afectado, es probable que puede tratarse de uno de los servicios que forman parte de RDS al sustituirlo por una clave controlada por el atacante, lo que permitiría el escalamiento de privilegios para agregar nuevos usuarios al grupo de administradores, otorgando privilegios completos de SYSTEM.

CVSS: 3.1 / AV: L (Local) puntuación 7.8

V. IMPACTO

Producto	KB Articulo	Build Number
Windows Server 2025	KB5075899, KB5075942	10.0.26100.32370
Windows 11 24H2 (x64/ARM64)	KB5077181, KB5077212	10.0.26100.7840
Windows Server 2022	KB5075906, KB5075943	10.0.20348.4773
Windows 11 23H2 (x64/ARM64)	KB5075941	10.0.22631.6649
Windows Server 2019	KB5075904	10.0.17763.8389
Windows 10 22H2 (various)	KB5075912	10.0.19045.6937
Windows Server 2016	KB5075999	10.0.14393.8868
Windows Server 2012 R2	KB5075970	6.3.9600.23022

Tabla 1.- Productos Afectados - Vulnerabilidad 0-Day CVE-2026-21533 en Windows RDS (Elevación de Privilegios)

VI. INDICADORES DE COMPROMISO

Entre los IoC, se tiene:

- Modificación de una clave (KEY) de configuración de un servicio, normalmente implica cambios en el Registro de Windows.
- La creación de nuevas cuentas de usuario de tipo ADMIN en Windows.
- Procesos ejecutándose como SYSTEM.
- Conexión RDP sospechosa.

VII. RECOMENDACIONES:

- Deshabilitar RDS si no se utiliza; restringir a redes de confianza.

- Hacer cumplir menos privilegios; supervisar los cambios de registro en los servicios de RDS.
- Implemente EDR para escaladas de privilegios anómalas.
- Prueba los parches en entornos de prueba debido a la sensibilidad de RDS.

VIII. 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.

IX. REFERENCIAS:

CYBERSECURITY NEWS (2026). Windows Remote Desktop Services 0-Day Vulnerability. https://cybersecuritynews.com/windows-remote-desktop-services-0-day-vulnerability/

MICROSOFT SECURITY RESPONSE CENTER (2026). CVE-2026-21533 – Microsoft Vulnerability Update Guide.
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21533

HISPASEC UNAALDIA (2026). CISA advierte sobre seis nuevos 0-day críticos en Microsoft tras explotación activa.
https://unaaldia.hispasec.com/2026/02/cisa-advierte-sobre-seis-nuevos-0-day-criticos-en-microsoft-tras-explotacion-activa.html

CVE DETAILS (2026). CVE-2026-21533 Detail.
https://www.cvedetails.com/cve/CVE-2026-21533/

MICROSOFT SECURITY RESPONSE CENTER (2026). Advisory: CVE-2026-21533 (inglés). https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2026-21533