Microsoft ha lanzado sus nuevas actualizaciones de seguridad con las que se pueden solucionar todas las vulnerabilidades detectadas en Windows, y demás productos de software.

En esta ocasión, Microsoft ha lanzado un total de 66 actualizaciones de seguridad tanto para Windows como para otros productos de la propia compañía, y al mismo tiempo, junto a estos parches se pueden identificar 3 actualizaciones para productos que no son de Microsoft, como, por ejemplo, Chromium.

La mayoría de las vulnerabilidades se han registrado con un nivel de severidad «importante», excepto dos, que se han catalogado como «críticas» al tratarse de dos fallos de día cero muy peligrosos. Uno de ellos se encuentra en el protocolo SMB, el cual permite escalar privilegios dentro del sistema hasta conseguir su máximo nivel: "SYSTEM". Esta amenaza, combinada con el segundo 0-day, en el protocolo WEBDAV, consigue ejecutar código remoto en el sistema con el máximo nivel de privilegios.

Versiones de Windows actualizadas:

Windows 10:
21H2
22H2
Windows 11:
22H2
23H2
24H3

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Las vulnerabilidades críticas más destacadas incluyen ejecución remota de código en Windows Schannel (CVE-2025-29828), en los Servicios de Escritorio Remoto de Windows (CVE-2025-32710) y en Microsoft Office (CVE-2025-47162, CVE-2025-47953, CVE-2025-47164 y CVE-2025-47167), así como elevación de privilegios en Power Automate (CVE-2025-47966).

Se ha observado explotación activa de la zero-day CVE-2025-33053 en WEBDAV.

Clasificación de las vulnerabilidades según su descripción:

- 25 vulnerabilidades de ejecución remota de código.
- 17 vulnerabilidades de divulgación de información.
- 13 vulnerabilidades de elevación de privilegios.
- 6 vulnerabilidades de denegación de servicio.
- 3 vulnerabilidades de bypass de funciones de seguridad.
- 2 vulnerabilidades de suplantación.

Recursos afectados:

- Windows Storage Management Provider
- Windows Cryptographic Services
- .NET and Visual Studio
- Windows Remote Desktop Services
- Windows Win32K – GRFX
- Windows Common Log File System Driver
- Windows Installer
- Remote Desktop Client
- Windows Media

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Windows SMB
- Windows Recovery Driver
- Windows Storage Port Driver
- Windows Local Security Authority Subsystem Service (LSASS)
- Windows DHCP Server
- Windows DWM Core Library
- WebDAV
- Microsoft Local Security Authority Server (lsasrv)
- Windows Local Security Authority (LSA)
- Windows Routing and Remote Access Service (RRAS)
- Windows Kernel
- Windows Standards-Based Storage Management Service
- App Control for Business (WDAC)
- Windows Netlogon
- Windows KDC Proxy Service (KPSSVC)
- Windows Shell
- Microsoft Office
- Microsoft Office SharePoint
- Microsoft Office Excel
- Microsoft Office Word
- Microsoft Office Outlook
- Microsoft Office PowerPoint
- Windows Remote Access Connection Manager
- Windows Security App
- Visual Studio

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Windows SDK
- Power Automate
- Microsoft AutoUpdate (MAU)
- Windows Hello
- Nuance Digital Engagement Platform

Detalle de las vulnerabilidades críticas:

CVE-2025-47172: Vulnerabilidad de Ejecución Remota de Código en el Servidor Microsoft SharePoint

- Severidad: Crítica
- CVSS: 8.8
- Divulgación: No
- Explotación: No detectada
- Explotación última versión: Poco probable
- Soluciones alternativas: No

CVE-2025-47162: Vulnerabilidad de Ejecución Remota de Código en Microsoft Office

- Severidad: Crítica
- CVSS: 8.4
- Divulgación: No
- Explotación: No detectada
- Explotación última versión: Probable
- Soluciones alternativas: No

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

CVE-2025-29828: Vulnerabilidad de Ejecución Remota de Código en Windows Schannel

- Severidad: Crítica
- CVSS: 8.1
- Divulgación: No
- Explotación: No detectada
- Explotación última versión: Poco probable
- Soluciones alternativas: No

CVE-2025-32710: Vulnerabilidad de Ejecución Remota de Código en los Servicios de Escritorio Remoto de Windows

- Severidad: Crítica
- CVSS: 8.1
- Divulgación: No
- Explotación: No detectada
- Explotación última versión: Poco probable
- Soluciones alternativas: No

CVE-2025-33071: Vulnerabilidad de Ejecución Remota de Código en el Servicio de Proxy KDC de Windows (KPSSVC)

- Severidad: Crítica
- CVSS: 8.1
- Divulgación: No
- Explotación: No detectada
- Explotación última versión: Probable

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

- Soluciones alternativas: No

CVE-2025-33070: Vulnerabilidad de Elevación de Privilegios de Netlogon en Windows

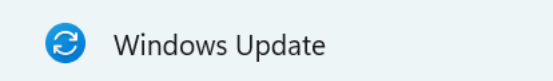
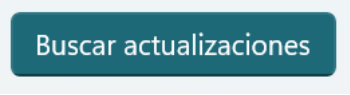
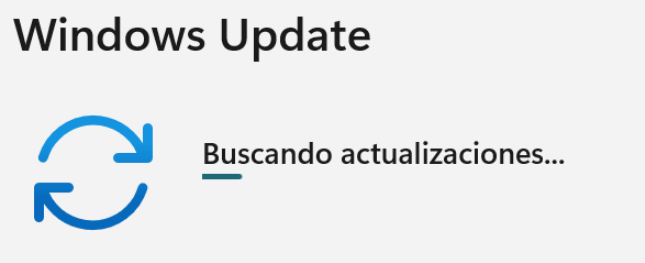
- Severidad: Crítica
- CVSS: 8.1
- Divulgación: No
- Explotación: No detectada
- Explotación última versión: Probable
- Soluciones alternativas: No

Recomendaciones:

- Se recomienda aplicar las actualizaciones de seguridad más recientes de Microsoft en todos los sistemas afectados, con los nuevos parches disponibles desde Windows update.
- Actualizar sistemas con parches oficiales.
- Capacitación al personal para evitar vectores de explotación.

Pasos para la actualización de Microsoft:

Acción	Ilustración
Abrir botón inicio	
Selecciona Configuración (Settings).	

Acción	Ilustración
Dentro del panel de Configuración, haz clic en 'Actualización y seguridad' o (Update & Security) o Windows Update	
En la pestaña 'Windows Update', haz clic en 'Buscar actualizaciones' (Check for updates).	
Inmediatamente se buscaran las actualizaciones de forma automática	
Una vez encontrada las actualizaciones pendientes se debe seleccionar descargar e instalar o instalar ahora	

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570

Acción	Ilustración
Verificar que el sistema esté actualizado	

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 316 8931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

Fuentes:

- https://www.softzone.es/noticias/windows/parches-seguridad-junio-2025/
- https://ciberseguridad.euskadi.eus/noticia/2025/actualizacion-de-seguridad-de-microsoft-junio-2025/webcyb00-contcibglos/es/#:~:text=En%20junio%20de%202025%2C%20Microsoft,2%20corresponden%20a%20zero%2Dday
- https://msrc.microsoft.com/update-guide
- https://msrc.microsoft.com/update-guide/vulnerability

CSIRT Salud
Dirección: Calle 119 No. 13 – 51
Bogotá D.C., Colombia
Tel: (+57) 3168931490 – 3181553570