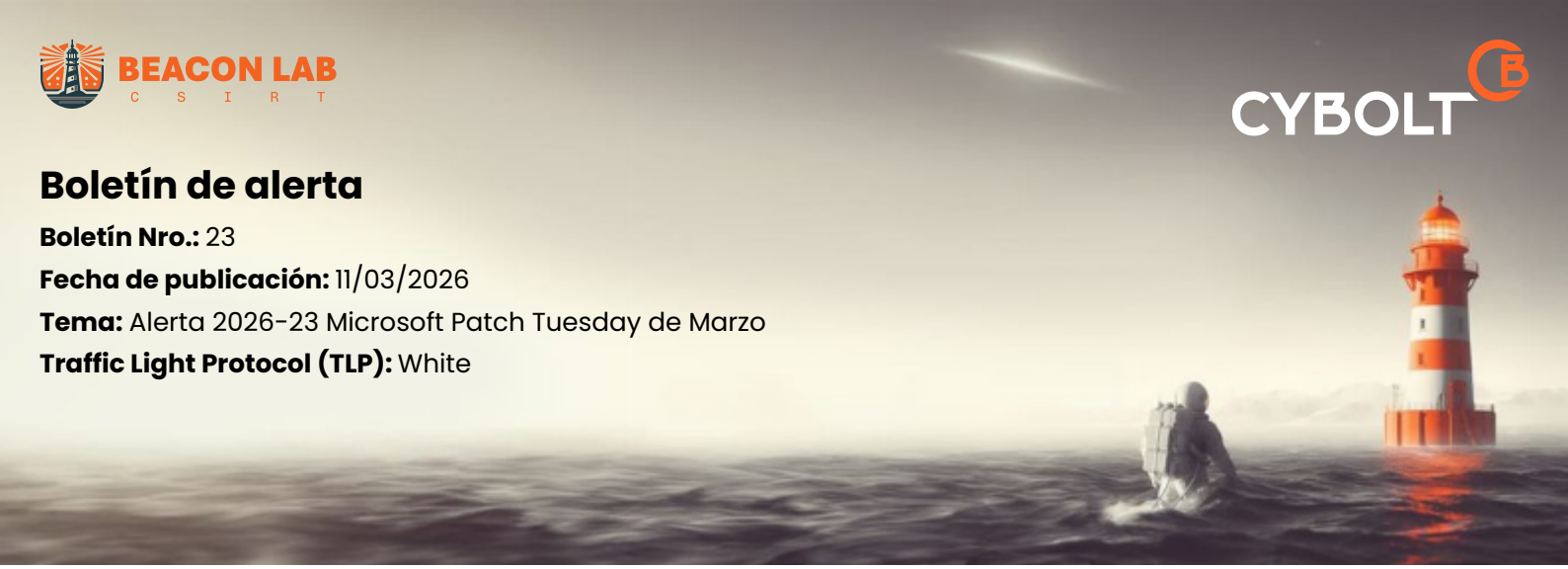

Boletín de alerta

Boletín Nro.: 23
Fecha de publicación: 11/03/2026
Tema: Alerta 2026-23 Microsoft Patch Tuesday de Marzo
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Las vulnerabilidades corregidas afectan múltiples productos y componentes del ecosistema Microsoft, incluyendo:

- **Microsoft Windows (Windows 10, Windows 11 y versiones de Windows Server compatibles)**
- **Microsoft Office y Microsoft Office Services**
- **Microsoft Edge (Chromium-based)**
- **Windows Kernel**
- **Windows Remote Desktop Services**
- **Windows NTLM y componentes de autenticación**
- **Windows Installer**
- **Windows Storage**
- **Windows Hyper-V**
- **Windows Graphics Component**
- **Windows Defender y otros componentes de seguridad del sistema**

Descripción

Recientemente, Microsoft publicó su Patch Tuesday correspondiente a marzo de 2026, abordando **84 vulnerabilidades de seguridad** presentes en distintos productos de su ecosistema, principalmente en Windows y servicios asociados. De acuerdo con el Microsoft Security Response Center (MSRC) y diversos análisis de seguridad, **8 de estas vulnerabilidades han sido clasificadas como críticas**, mientras que **76 están catalogadas con severidad "Important"**.

Entre las fallas corregidas se incluyen **46 vulnerabilidades de elevación de privilegios**, **18 de ejecución remota de código (RCE)**, **10 de divulgación de información**, además de **4 de suplantación (spoofing)**, **4 de denegación de servicio (DoS)** y **2 de bypass de mecanismos de seguridad**. Las vulnerabilidades de **elevación de privilegios representan la mayor parte de los fallos**, lo que indica que muchos ataques podrían aprovechar estas debilidades después de obtener acceso inicial al sistema para escalar privilegios y comprometer completamente el host.

Entre las CVEs críticas más destacadas están:

- **CVE-2026-21915** – Windows Remote Desktop Services Remote Code Execution

Esta vulnerabilidad permite **ejecución remota de código** en sistemas que utilizan **Remote Desktop Services** debido a un manejo incorrecto de solicitudes enviadas al servicio RDP. Un atacante remoto podría enviar paquetes especialmente diseñados al sistema vulnerable y lograr la ejecución de código arbitrario con privilegios elevados, lo que podría derivar en la instalación de malware, control del sistema o movimiento lateral dentro de una red corporativa, especialmente en entornos donde RDP se encuentra expuesto a Internet.

- **CVE-2026-21918** – Windows NTLM Authentication Remote Code Execution

Esta falla afecta el mecanismo de **autenticación NTLM** en Windows y podría permitir a un atacante ejecutar código mediante el procesamiento de solicitudes de autenticación manipuladas. La explotación podría facilitar el compromiso de sistemas al abusar del proceso de autenticación, lo que abre la posibilidad de ataques relacionados con **relay, robo de credenciales o escalamiento de privilegios**, particularmente en entornos corporativos que todavía dependen de NTLM por compatibilidad con sistemas heredados.

- **CVE-2026-21921** – Hyper-V Elevation of Privilege:

Esta vulnerabilidad impacta el hipervisor Hyper-V y permite que un atacante que ya tenga acceso a una máquina virtual pueda **elevar privilegios y potencialmente escapar del entorno virtualizado hacia el host** . La falla se origina por una gestión incorrecta de recursos durante la interacción entre la máquina virtual y el hipervisor, lo que podría comprometer el sistema anfitrión y otras máquinas virtuales en el mismo entorno, representando un riesgo significativo para infraestructuras de virtualización empresariales.

Solución y mitigaciones:

Microsoft recomienda aplicar **las actualizaciones de seguridad publicadas en el Patch Tuesday de marzo de 2026 lo antes posible**, especialmente en entornos empresariales donde los sistemas Windows se encuentran ampliamente desplegados. Las actualizaciones se distribuyen mediante **Windows Update, Windows Update for Business, WSUS y el Microsoft Update Catalog**.

Las actualizaciones oficiales y parches pueden consultarse en el portal del **Microsoft Security Update Guide**:
https://msrc.microsoft.com/update-guide

Además de aplicar los parches, se recomienda que las organizaciones implementen las siguientes medidas complementarias:

- Priorizar el parcheo en **servidores críticos y estaciones de trabajo expuestas a internet**.
- Aplicar **principio de mínimo privilegio** para reducir el impacto de vulnerabilidades de escalamiento de privilegios.

- Monitorear eventos de seguridad relacionados con **ejecución de código, cambios de privilegios y autenticaciones anómalas**.
- Utilizar soluciones de **EDR/XDR o SIEM** para detectar explotación activa de vulnerabilidades.

Información adicional:

- https://thehackernews.com/2026/03/microsoft-patches-84-flaws-in-march.html
- https://msrc.microsoft.com/update-guide
- https://zecurit.com/endpoint-management/patch-tuesday