USTIC-AV 21/22. Los parches de Microsoft Windows de diciembre corrigen 6 vulnerabilidades críticas (19/12/2022)

La **Unidad de Seguridad TIC** de la Subdirección de Tecnologías de la Información y Comunicaciones **avisa** de que han sido **liberados los parches de seguridad mensuales de Microsoft Windows de diciembre que corrigen,** entre otras, **6 vulnerabilidades críticas, incluidas 2 de día cero conocidas, una de las cuales estaba siendo explotada activamente**.

Asimismo, en el apartado correspondiente en este comunicado, se informa del **calendario del despliegue desde Altiris** de estos parches para puestos de usuarios.

Respecto a los servidores afectados, se ruega a sus responsables la máxima diligencia en su resolución, debido al riesgo potencial que presentan estas vulnerabilidades.

Detalle

Microsoft ha lanzado su nueva ronda de actualizaciones para Windows en su boletín mensual de diciembre, corrigiendo 79 vulnerabilidades, 6 de ellas clasificadas como críticas (dos son de Día Cero o *0-day*), ya que, alternativa o conjuntamente, permiten la elevación de privilegios del sistema, la suplantación de identidad o la ejecución remota de código

Entre las vulnerabilidades que resuelven las actualizaciones, habría que destacar las siguientes críticas de día cero:

- CVE-2022-44698: Vulnerabilidad de omisión de características de seguridad SmartScreen en Windows, en la que un atacante puede crear un archivo malicioso que evadiría las defensas de la Marca de la Web (MOTW), lo que resulta en una pérdida limitada de integridad y disponibilidad de características de seguridad como Vista protegida en Microsoft Office, que dependen del etiquetado MOTW.

  Los ciberdelincuentes vinculados al grupo de ransomware Magniber han explotado la vulnerabilidad de omisión de la función de seguridad en los ataques de extorsión y robo de datos.

- CVE-2022-44710: Vulnerabilidad de elevación de privilegios en el kernel de gráficos DirectX que podría ser aprovechado por un atacante para obtener privilegios de SYSTEM en un sistema comprometido.

Para un mayor conocimiento del resto de fallos de seguridad que arreglan estos parches, puede consultarse el boletín de la compañía.

Asimismo, debido al riesgo potencial que presentan estas vulnerabilidades, llamamos vuestra atención sobre la urgencia de aplicar las recomendaciones indicadas y la adopción de medidas tan pronto como sea posible.

Sistemas Afectados

- Windows 7.
- Windows 8.1
- Windows 10
- Windows 11.
- Windows Server 2008 y 2008 R2.
- Windows Server 2012 y 2012 R2.
- Windows Server 2016.
- Windows Server 2019.
- Windows Server 2022.

Recomendaciones Actualizadas (19/12/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones recomienda encarecidamente aplicar los siguientes pasos, con el fin de evitar la exposición a ataques externos y la toma de control de los sistemas informáticos:

Mitigación

1º. Solución a las vulnerabilidades:

Será necesario **implementar los parches** liberados lo antes posible.

Despliegue de Parches desde Altiris para Equipos de Usuarios. Calendario.

El despliegue de los parches de seguridad de los equipos de usuario se realizará desde Altiris de manera escalonada, por anillos, atendiendo al siguiente calendario:

- **Anillo 1**: 20 de diciembre
- **Anillo 2:** 27 de diciembre
- **Anillo 3**: 3 de enero

Desde el punto de vista del impacto en los usuarios, esta actualización, una vez instalada, informará al usuario que debe reiniciar el equipo.

Referencias

- Security Update Guide
- December 2022 Security Updates

Para cualquier duda o consulta al respecto, puede ponerse en contacto con nuestro equipo en ustic.stic.sspa@juntadeandalucia.es.

Gracias por vuestra atención.

Unidad de Seguridad TIC

Subdirección de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud