USTIC-AV 13/22. Corrección de 5 vulnerabilidades críticas y 2 de “día cero” con los parches de Microsoft Windows de septiembre (20/09/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones avisa de que han sido **l iberados los parches de seguridad mensuales de Microsoft Windows de septiembre que corrigen,** entre otras, **5 vulnerabilidades críticas y 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 septiembre, corrigiendo 79 vulnerabilidades, 5 de ellas clasificadas como críticas, ya que permiten la ejecución remota de código y, otras 2, ya conocidas por la compañía, de “Día Cero” (*0-day*), una de las cuales está siendo activamente explotada.

El número de vulnerabilidades en cada categoría se enumeran de la siguiente forma:

- 18 Vulnerabilidades de elevación de privilegios.
- 1 Vulnerabilidades de omisión de características de seguridad.
- 30 Vulnerabilidades de ejecución remota de código.
- 7 Vulnerabilidades de divulgación de información.
- 7 Vulnerabilidades de denegación de servicio.
- 16 Vulnerabilidades de *Chromium*.

Entre las vulnerabilidades que resuelven las actualizaciones, habría que destacar las siguientes:

- **Dos de día cero:**
  - CVE-2022-37969: Explotada activamente, se debe a un fallo de escalada de privilegios que afecta al controlador del sistema de archivos de registro común (CLFS) de Windows, que podría ser aprovechado por un atacante para obtener privilegios de SYSTEM en un sistema comprometido.
  - CVE-2022-23960: Conocida como *Spectre-BHB*, podría describirse como una vulnerabilidad de especulación de canal lateral en los procesadores ARM.
- **Cinco críticas:**
  - CVE-2022-34718 (puntuación CVSS: 9.8): Vulnerabilidad de ejecución remota de código TCP/IP de Windows.
  - CVE-2022-34721 (puntuación CVSS: 9.8): Extensiones del protocolo de intercambio de claves de Internet (IKE) de Windows. Vulnerabilidad de ejecución remota de código.
  - CVE-2022-34722 (puntuación CVSS: 9.8): Extensiones de protocolo de intercambio de claves de Internet (IKE) de Windows. Vulnerabilidad de ejecución remota de código.
  - CVE-2022-34700 (puntuación CVSS: 8.8): Vulnerabilidad de ejecución remota de código de Microsoft Dynamics 265 (local).
  - CVE-2022-35805 (puntuación CVSS: 8.8): Vulnerabilidad de ejecución remota de código de Microosft Dynamics 265 (local).

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 2012 y 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Recomendaciones Actualizadas (20/09/2022)

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 septiembre
- Anillo 2: 27 de septiembre
- Anillo 3: 4 de octubre

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

Referencias

- Web de parches: https://msrc.microsoft.com/update-guide
- *Release Notes*: https://msrc.microsoft.com/update-guide/releaseNote/2022-Sep

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