USTIC-AV 09/22. Corrección de 17 vulnerabilidades críticas con los parches de Microsoft Windows de agosto (12/08/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones, siguiendo las indicaciones facilitadas por AndalucíaCERT, avisa de que han sido **liberados los parches de seguridad mensuales de Microsoft Windows de agosto que corrigen 17 vulnerabilidades críticas**.

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 agosto, corrigiendo 121 vulnerabilidades, 17 de ellas clasificadas como críticas (dos son de Día Cero o *0-day*), ya que permiten la ejecución remota de código o la elevación de privilegios dentro del Sistema.

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

- 64 Vulnerabilidades de elevación de privilegios.
- 6 Vulnerabilidades de omisión de características de seguridad.
- 31 Vulnerabilidades de ejecución remota de código.
- 12 Vulnerabilidades de divulgación de información.
- 7 Vulnerabilidades de denegación de servicio.
- 1 Vulnerabilidad de suplantación de identidad.

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

- CVE-2022-34713: Esta vulnerabilidad de Día Cero (*0-day*), conocida como “Dogwalk” y explotada activamente, se debe a un fallo en la herramienta Microsoft Windows Support Diagnostic Tool (*MSDT*). Un atacante remoto puede aprovechar esta vulnerabilidad para realizar un escalamiento de privilegios en el sistema afectado.

Adicionalmente, el equipo de Microsoft ha parcheado otra vulnerabilidad de ejecución remota de código en el componente MSDT, si bien no se tiene constancia de que esté siendo explotada actualmente: CVE-2022-35743.

En este sentido, no queremos dejar pasar la ocasión sin indicar que estas dos vulnerabilidades son distintas a *Follina* (CVE-2022-30190), que también afectaba al mismo componente, y de la que avisamos el pasado 3 de junio de 2022 aquí: https://ws001.sspa.juntadeandalucia.es/confluence/x/HZS3Bg .

- CVE-2022-30134: Se trata de la otra vulnerabilidad de Día Cero (*0-day*) que se debe a un error en el control de datos de entrada de Microsoft Exchange. Un atacante remoto podría acceder a mensajes de correo electrónico específicos.
- CVE-2022-34691: Calificada como crítica, esta vulnerabilidad se debe a un fallo en los servicios de Active *Directory* . Un atacante podría aprovechar esta vulnerabilidad para realizar un escalamiento de privilegios en el sistema afectado.
- CVE-2022-30133: Vulnerabilidad crítica de ejecución remota de código en el protocolo /Point-to-Point/ (PPP) de Windows

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 8.1
- Windows 10
- Windows Server 2012 y 2012 R2
- Windows Server 2016
- Windows Server 2019

Recomendaciones Actualizadas (12/08/2022)

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 para Windows 8.1 y Windows 10 de los equipos de usuario se realizará desde Altiris de manera escalonada, por anillos, atendiendo al siguiente calendario:

- Anillo 1: 16 agosto
- Anillo 2: 23 agosto
- Anillo 3: 30 agosto

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

Otras Cuestiones de Seguridad

Por último, queremos aprovechar para informar de que se va a desplegar en todos los terminales ligeros (LetSAS 6) el cliente de EDR, coincidiendo con el calendario de anillos detallado anteriormente.

Referencias

- Web de parches: https://msrc.microsoft.com/update-guide
- Release Notes: https://msrc.microsoft.com/update-guide/releaseNote/2022-Aug
- Ejecución remota de código en MSDT (CVE-2022-34713): https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34713
- Ejecución remota de código en MSDT (CVE-2022-35743): https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35743
- Aviso emitido por la USTIC sobre la vulnerabilidad Follina (CVE-2022-30190): https://ws001.sspa.juntadeandalucia.es/confluence/x/HZS3Bg
- Elevación de privilegios en Exchange (CVE-2022-21980): https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21980
- Elevación de privilegios en Exchange (CVE-2022-24477): https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24477
- Elevación de privilegios en Exchange (CVE-2022-24516): https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24516
- Revelación de información en Exchange (CVE-2022-30134): https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30134
- Elevación de privilegios en Active Directory Domain Services (CVE-2022-34691): https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-34691
- Ejecución remota de código en el protocolo PPP (CVE-2022-30133): https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30133

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