BOLETÍN DE ALERTA

Boletín Nro.: 2023-09
Fecha de publicación: 16/03/2023
Tema: Vulnerabilidad de escalamiento de privilegios explotada activamente en Microsoft

Los softwares afectados son:

- Microsoft Outlook 2013 service pack 1 (ediciones de 32 y 64 bits).
- Microsoft Outlook 2013 RT Service Pack 1.
- Microsoft Outlook 2016 (ediciones de 32 y 64 bits).
- Microsoft Outlook 2019 (ediciones de 32 y 64 bits).
- Microsoft Office LTSC 2021 (ediciones de 32 y 64 bits).
- Microsoft 365 Apps for Enterprise (ediciones de 32 y 64 bits).

Descripción:

Se han reportado nuevos avisos de seguridad sobre múltiples vulnerabilidades, incluidas dos de Día Cero (*0-day*) que afectan a productos de Microsoft, que permitirían a un atacante realizar escalamiento de privilegios, ejecución remota de código (*RCE*), denegación de servicio (*DoS*), entre otros.

Las vulnerabilidades corregidas se componen de 9 (nueve) de severidad "Crítica", 70 (setenta) de severidad "Alta", 1 (una) de severidad "Media" y 29 (veintinueve) sin severidad asignada aún. La principal de día cero (*0-day*) que está siendo explotada se detalla a continuación:

La vulnerabilidad identificada como CVE-2023-23397, de severidad "Crítica" y con puntuación de 9.8. Esta vulnerabilidad de Día Cero (*0-day*) se debe a una falla de filtración del *hash Net-NTLMv2* en Microsoft Outlook. Esto permitiría a un atacante remoto a través del envío de correos especialmente diseñados forzar al dispositivo a conectarse a una dirección *URL* remota para transmitir el *hash Net-NTLMv2* de la cuenta de Windows y obtener escalamiento de privilegios en el sistema afectado. Se recomienda actualizar los más pronto posible los productos afectados dado que se reporta que dicha vulnerabilidad está siendo explotada activamente.

Nota: Según Microsoft esta falla se activará antes de leer el correo en el **Panel de vista previa**, ya que la vulnerabilidad se activa automáticamente cuando el servidor de correo electrónico obtiene el correo malicioso de su base de datos local y lo procesa.

Adicionalmente, puede acceder al listado completo de vulnerabilidades ingresando aquí.

Impacto:

La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto realizar escalamiento de privilegios y provocar robo de correos electrónicos de cuentas específicas.

Solución:

Recomendamos instalar las actualizaciones correspondientes provistas por el fabricante a través de la siguiente guía:

- https://msrc.microsoft.com/update-guide
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397

Nota: Para los usuarios que cuenten con Windows Server 2008 R2 o Windows Server 2008 alojados en Azure, deben adquirir el **Extended Security Update** para seguir recibiendo las actualizaciones de seguridad. Para más información acceder al siguiente enlace.

Mitigación:

Adicionalmente, como medida de mitigación se recomienda tener en cuenta los siguientes factores importantes que podrían ser útiles:

1. Agregar usuarios al **Protected Users Security Group**, para impedir el uso de *NTLM* como mecanismo de autenticación. Considerar utilizarlo especialmente para cuentas privilegiadas, como administradores de dominio.

Nota: Se debe tener en cuenta que puede afectar a las aplicaciones que requieren el uso de los protocolos *NTLM*, sin embargo, la configuración se revertirá una vez que el usuario sea removido del grupo **Protected Users Security Group**. Para obtener más información consultar el siguiente enlace.

2. Bloquear el tráfico *TCP 445/SMB* saliente de la red mediante un firewall perimetral, un firewall local y/o mediante la configuración de *VPN*. Esto con el fin de evitar el envío de mensajes *NTLM* a recursos compartidos de servidores remotos.

Información adicional:

- https://www.bleepingcomputer.com/news/microsoft/microsoft-march-2023-patch-tuesday-fixes-2-zero-days-83-flaws/
- https://thehackernews.com/2023/03/microsoft-rolls-out-patches-for-80-new.html
- https://nvd.nist.gov/vuln/detail/CVE-2023-23397
- https://msrc.microsoft.com/update-guide/
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397
- https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group