BOLETÍN DE ALERTA

Boletín Nro.: 2023-42
Fecha de publicación: 13/09/2023
Tema: Vulnerabilidades de escalamiento de privilegios y divulgación de información en productos Microsoft

Principales softwares afectados:

- Windows Server 2022.
- Windows Server 2019 (Server Core installation).
- Windows 10 Version 22H2 for 32-bit Systems.
- Microsoft Word 2013 RT Service Pack 1.
- Microsoft Word 2016 (64-bit edition).
- Microsoft 365 Apps for Enterprise for 64-bit Systems.

Se puede acceder al listado completo de productos afectados aquí

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre dos vulnerabilidades *Zero Day* que afectan a productos Microsoft, que permitirían a un atacante realizar escalamiento de privilegios y divulgación de información del sistema afectado.

Las vulnerabilidades corregidas se componen de 1 (una) de severidad "Alta" y 1 (una) de severidad "Media". Las mismas se detallan a continuación:

- CVE-2023-36802, de severidad "Alta" y con puntuación de 7.8. Esta vulnerabilidad *Zero Day* con explotación detectada, se debe a una falla de seguridad en Microsoft Streaming Service Proxy. Esto permitiría a un atacante realizar escalamiento de privilegios y obtener privilegios de *SYSTEM* en el sistema afectado.

- CVE-2023-36761, de severidad "Media" y con puntuación de 6.2. Esta vulnerabilidad *Zero Day* con explotación detectada, se debe a una falla de seguridad en Microsoft Word. Esto permitiría a un atacante a través del panel de vista previa, realizar divulgación de información y de *hashes NTLM* del sistema afectado.

Impacto:

La explotación exitosa de estas vulnerabilidades podría permitir a un atacante realizar escalamiento de privilegios y divulgación de información del sistema afectado.

Solución:

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

- https://msrc.microsoft.com/update-guide

Información adicional:

- https://www.securityweek.com/zero-day-summer-microsoft-warns-of-fresh-new-software-exploits/
- https://nvd.nist.gov/vuln/detail/CVE-2023-36802
- https://nvd.nist.gov/vuln/detail/CVE-2023-36761
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36802
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36761
- https://msrc.microsoft.com/update-guide