BOLETÍN DE ALERTA

Boletín Nro.: 2023-36
Fecha de publicación: 10/08/2023
Tema: Actualizaciones de seguridad para productos Microsoft

Principales softwares afectados son:

- Microsoft Exchange Server.
- Microsoft Office.
- Windows Kernel.
- Azure HDInsights.
- Windows Defender.

Adicionalmente, puede acceder al listado completo de software afectado ingresando aquí.

Descripción:

Se han lanzado actualizaciones de seguridad relacionadas a múltiples vulnerabilidades, incluidas dos *Zero Day* que afectan a productos Microsoft, que permitirían a un atacante realizar ejecución remota de código (*RCE*), escalamiento de privilegios, denegación de servicios (*DoS*), entre otros.

Las vulnerabilidades corregidas se componen de 4 (cuatro) de severidad "Crítica", 47 (cuarenta y siete) de severidad "Alta" y 25 (veinticinco) de severidad "Media. Las principales se detallan a continuación:

- CVE-2023-21709, de severidad "Crítica" y con puntuación de 9.8. Esta vulnerabilidad se debe a una falla de seguridad en Microsoft Exchange Server. Esto permitiría a un atacante no autenticado realizar ataques de fuerza bruta desde la red contra cuentas de usuarios válidas con el fin de iniciar sesión y realizar escalamiento de privilegios en el sistema afectado.

- CVE-2023-35385, CVE-2023-36910 y CVE-2023-36911, de severidad "Critica" y con puntuación de 9.8. Estas vulnerabilidades se deben a fallas en el componente Microsoft Message Queuing (*MSMQ*). Un atacante remoto no autenticado podría explotar esta vulnerabilidad mediante el envío de paquetes *MSMQ* especialmente diseñados y realizar ejecución de código arbitrario en el servidor afectado.

- CVE-2023-38185, de severidad “Alta” y con puntuación de 8.8. Esta vulnerabilidad se debe a una falla de seguridad en Microsoft Exchange Server. Esto permitiría a un atacante autenticado a través de una llamada de red desencadenar código malintencionado en el contexto y provocar ejecución remota de código (*RCE*) en el sistema afectado.

- CVE-2023-36884, de severidad “Alta” y con puntuación de 8.8. Esta vulnerabilidad *Zero Day* que está siendo explotada activamente, especialmente a través del envío de mensajes de correo electrónico, se debe a una falla en el componente de búsqueda de Windows. Un atacante remoto podría enviar un documento de Microsoft Office especialmente diseñado para realizar ejecución remota de código (*RCE*) en el sistema afectado.

- CVE-2023-35388 y CVE-2023-38182, ambas de severidad “Alta” y con puntuación de 8.0. Estas vulnerabilidades se deben a una falla de seguridad en Microsoft Exchange Server. Esto permitiría a un atacante autenticado y en la misma red a través de una sesión remota de comunicación de *PowerShell*, realizar ejecución remota de código (*RCE*) en el sistema afectado.

- CVE-2023-38180, de severidad “Alta” y con puntuación de 7.5. Esta vulnerabilidad *Zero Day* con *PoC* publica que está siendo explotada activamente se debe a una falla de seguridad en los componentes .NET y Visual Studio. Esto permitiría a un atacante provocar ataques de denegación de servicios (*DoS*) en el sistema afectado.

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

Impacto:

La explotación exitosa de estas vulnerabilidades podría permitir a un atacante realizar ejecución remota de código (*RCE*), escalamiento de privilegios, denegación de servicios (*DoS*), entre otros.

Solución:

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

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

Mitigación:

Adicionalmente, como medida de mitigación para la vulnerabilidad CVE-2023-21709 se recomienda seguir uno de los siguientes pasos:

1. Instalar Exchange Server 2016 o 2019 August SU (o posterior) (recomendado)
2. O realizar una de las siguientes acciones:

    - Aplicar la actualización automáticamente en los servidores y ejecutar el *script* *CVE-2023-21709.ps1*.
      OBS: Este script debe ejecutarse como administrador en Exchange Management Shell (*EMS*).

    - Aplicar la actualización manualmente en cada servidor, ejecutando el siguiente comando desde una ventana de *PowerShell* con privilegios elevados:

      ```
      Clear-WebConfiguration-Filter
      "/system.webServer/globalModules/add[@name='TokenCacheModule']" -PSPath
      "IIS:\"
      ```

      OBS: Para revertir manualmente la solución para el CVE en cada servidor, ejecutar lo siguiente:

      ```
      New-WebGlobalModule -Name "TokenCacheModule" -Image
      "%windir%\System32\inetsrv\cachtokn.dll"
      ```

Información adicional:

- https://www.bleepingcomputer.com/news/microsoft/microsoft-august-2023-patch-tuesday-warns-of-2-zero-days-87-flaws/
- https://msrc.microsoft.com/update-guide/releaseNote/2023-Aug
- https://nvd.nist.gov/vuln/detail/CVE-2023-21709
- https://nvd.nist.gov/vuln/detail/CVE-2023-38180
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21709
- https://msrc.microsoft.com/update-guide/vulnerability/ADV230003
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38180
- https://msrc.microsoft.com/update-guide
- https://thehackernews.com/2023/08/microsoft-releases-patches-for-74-new.html