BOLETÍN DE ALERTA

Boletín Nro.: 2023-19
Fecha de publicación: 11/05/2023
Tema: Actualizaciones de seguridad para productos Microsoft

Principales softwares afectados son:

- Windows Server 2012 R2 (Server Core installation).
- Windows 10 Versión 21H2 (ediciones de 32 y 64 bits).
- Windows Server 2012.
- Windows Server 2016.
- Windows Server 2019.
- Windows Server 2022 (Server Core installation).

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

Descripción:

Microsoft ha lanzado actualizaciones de seguridad relacionadas a múltiples vulnerabilidades, incluyendo un *0-day*, que afectan a varios de sus productos, que permitirían a un atacante remoto realizar ejecución remota de código (*RCE*), escalamiento de privilegios, entre otros.

Las vulnerabilidades corregidas se componen de 2 (dos) de severidad "Crítica", 26 (veintiséis) de severidad "Alta", 9 (nueve) de severidad "Media" y 1 (uno) de severidad "Baja". Las principales se detallan a continuación:

- CVE-2023-24943, de severidad "Crítica" y con puntuación de 9.8. Esta vulnerabilidad se debe a una falla de seguridad en *Windows Pragmatic General Multicast (PGM)*. Esto permitiría a un atacante enviar un archivo especialmente diseñado a través de la red al momento en el que el servicio Windows Message Queuing se ejecuta en un entorno de *PGM* Server, provocando la ejecución remota de código (*RCE*) en el sistema afectado.

- CVE-2023-24941, de severidad "Crítica" y con puntuación de 9.8. Esta vulnerabilidad se debe a una falla de seguridad en *Network File System (NFS)*. Esto permitiría a un atacante enviar una solicitud especialmente diseñada a través de la red a un servicio de *Network File System (NFS)*, provocando la ejecución remota de código (*RCE*) en el sistema afectado.

- CVE-2023-29336, de severidad “Alta”, con una puntuación asignada de 7.8. Esta vulnerabilidad de día cero (*0-day*) que está siendo explotada activamente se debe a una falla de seguridad en *Win32k*. Esto permitiría a un atacante provocar escalamiento de privilegios a *SYSTEM* en el sistema afectado.

Adicionalmente, puede acceder al listado completo de 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-2023-24941 se recomienda tener en cuenta los siguientes pasos:

1. Antes de actualizar la versión de Windows que protege contra esta vulnerabilidad, se puede mitigar el ataque deshabilitando *NFSV4.1*. Esto podría afectar negativamente a fututo y solo se recomienda aplicar la medida como una mitigación temporal, esta vulnerabilidad no afecta en *NFSV2.0* o *NFSV3.0*.

Nota: No se debe aplicar esta mitigación a menos que ya se haya instalado las actualizaciones de seguridad de Windows de mayo de 2022.

2. El siguiente comando de *PowerShell* deshabilitará la versión:

```
PS C:\Set-NfsServerConfiguration -EnableNFSV4 $false
```

3. Después de ejecutar el comando, se debe reiniciar el servidor *NFS* o reiniciar la máquina.
4. Para reiniciar el servidor *NFS*, iniciar la ventana *cmd* con **Ejecutar como administrador** y escribir los siguiente:
   - Detención del servidor **NFSADMIN**
   - Inicio del servidor **NFSADMIN**
5. Para confirmar que *NFSv4.1* se ha desactivado, se debe ejecutar el siguiente comando en una ventana de *PowerShell*:

```
PS C:\Get-NfsServerConfiguration
```

6. En la salida se puede observar que EnableNFSv4.1 es "False" ahora:

```
State : Running
LogActivity :
CharacterTranslationFile : Not Configured
DirectoryCacheSize (KB) : 128
HideFilesBeginningInDot : Disabled
EnableNFSV2 : True
EnableNFSV3 : True
EnableNFSV4 : False
EnableAuthenticationRenewal : True
AuthenticationRenewalIntervalSec : 600
NlmGracePeriodSec : 45
MountProtocol : {TCP, UDP}
NfsProtocol : {TCP, UDP}
NisProtocol : {TCP, UDP}
NlmProtocol : {TCP, UDP}
NsmProtocol : {TCP, UDP}
PortmapProtocol : {TCP, UDP}
MapServerProtocol : {TCP, UDP}
PreserveInheritance : False
NetgroupCacheTimeoutSec : 30
UnmappedUserAccount :
WorldAccount : Everyone
AlwaysOpenByName : False
GracePeriodSec : 240
LeasePeriodSec : 120
OnlineTimeoutSec : 180
```

7. Para volver a habilitar *NFSv4.1* después de haber instalado la actualización de seguridad, se debe escribir el siguiente comando:

```
Set-NfsServerConfiguration -EnableNFSV4 $True
```

8. Nuevamente, después de ejecutar el comando, se deberá reiniciar el servidor *NFS* o reiniciar la computadora.

Información adicional:

- https://thehackernews.com/2023/05/microsofts-may-patch-tuesday-fixes-38.html
- https://nvd.nist.gov/vuln/detail/CVE-2023-24941
- https://nvd.nist.gov/vuln/detail/CVE-2023-24943
- https://nvd.nist.gov/vuln/detail/CVE-2023-29336
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24941
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24943
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29336
- https://msrc.microsoft.com/update-guide/releaseNote/2023-May
- https://msrc.microsoft.com/update-guide