BOLETÍN DE ALERTA

Boletín Nro.: 2022-31
Fecha de publicación: 15/07/2022
Tema: Vulnerabilidad de ejecución remota de código (*RCE*) en Network File System de Windows

Productos afectados:

- Network File System, versión 4.1
- Windows Server 2012, 2012 R2
- Windows Server 2016
- Windows Server 2019

Descripción:

Se ha reportado una vulnerabilidad crítica en *Network File System de Windows*, que permitiría a un atacante realizar ejecución remota de código (*RCE*) en el sistema afectado.

La vulnerabilidad identificada como CVE-2022-30136 de severidad crítica y puntuación de 9.8. Esta vulnerabilidad se debe a un error en la implementación de Network File System (*NFS*) con relación al manejo incorrecto de las solicitudes *NFS*v4. Un atacante remoto puede aprovechar esta vulnerabilidad enviando llamadas RPC maliciosas a un servidor de destino.

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría a un atacante no autenticado realizar ejecución remota de código (*RCE*) en el sistema afectado.

Mitigación:

Esta vulnerabilidad no se puede explotar en NFS en sus versiones NFSV2.0 o NFSV3.0, por lo tanto, si aún no es posible la actualización del Windows, mientras tanto es posible mitigar esta vulnerabilidad deshabilitando el NFS en su versión NFSV4.1. Esto podría afectar negativamente a su entorno tecnológico y solo debe usarse como una mitigación temporal.

Advertencia: NO debe aplicar esta mitigación a menos que haya instalado las actualizaciones de seguridad de Windows de mayo del 2022, debido a que estas últimas subsanan una vulnerabilidad crítica que afecta a las versiones NFSV2.0 y NFSV3.0.

El siguiente comando de PowerShell deshabilitará esas versiones:

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

Después de ejecutar el comando, deberá reiniciar el servidor NFS o reiniciar la máquina.

Para reiniciar el servidor *NFS*, inicie una ventana **cmd** con la opción **Ejecutar como administrador**, y para ello escriba los siguientes comandos:

```
nfsadmin server stop
nfsadmin server start
```

Para confirmar que *NFS*v4.1 se ha desactivado, ejecute el siguiente comando en una ventana de Powershell:

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

Aquí está el resultado de la muestra. Observe que Enable*NFS*v4.1 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
```

Para volver a habilitar *NFS*v4.1 después de haber instalado la actualización de seguridad de junio de 2022, escriba el siguiente comando:

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

Una vez más, después de ejecutar el comando, deberá reiniciar el servidor *NFS* o reiniciar la máquina.

Adicionalmente, recomendamos acceder a las actualizaciones provistas por Microsoft en el siguiente enlace:

- https://support.microsoft.com/en-us/windows/get-the-latest-windows-update-7d20e88c-0568-483a-37bc-c3885390d212#WindowsVersion=Windows_11

Información adicional:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30136
- https://nvd.nist.gov/vuln/detail/CVE-2022-30136
- https://support.microsoft.com/en-us/windows/get-the-latest-windows-update-7d20e88c-0568-483a-37bc-c3885390d212#WindowsVersion=Windows_11