USTIC-AV 01/22. Vulnerabilidad crítica en Samba. (03/02/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones, siguiendo las indicaciones marcadas por el Equipo de Respuesta a Incidentes del Centro Criptológico Nacional, CCN-CERT, avisa de la publicación de una **vulnerabilidad** calificada como **crítica** que afecta a **Samba**.

Se ha dado a conocer una vulnerabilidad en Samba, una popular implementación de código abierto del protocolo Server Message Block (SMB) que permite la interconexión de redes Windows, Linux y UNIX, entre otros sistemas operativos. **Este fallo puede** llegar a permitir **ejecutar código de forma remota** (RCE)

La vulnerabilidad ha sido catalogada con el **CVE-2021-44142** y calificada como crítica. Se trata de un fallo de lectura /escritura fuera de límites y afecta al módulo VFS Samba (vfs_fruit), diseñado para mejorar la compatibilidad entre los clientes SMB de Apple y los servidores de archivos Netatalk 3 AFP. Un atacante remoto con la capacidad de escribir en los atributos extendidos del archivo puede desencadenar una escritura fuera de los límites y ejecutar código arbitrario con privilegios de administrador.

Actualmente no se tiene conocimiento de reportes sobre actividad dañina en la red ni de la disponibilidad de exploits que aprovechen esta vulnerabilidad, así como tampoco, se han publicado pruebas de concepto (PoC) de la vulnerabilidad.

Debido a la criticidad alta de esta vulnerabilidad rogamos encarecidamente que se sea especialmente diligente en su resolución. Llamamos vuestra atención sobre la necesidad de aplicar las recomendaciones indicadas y la adopción de medidas para hacer frente a la vulnerabilidad.

Recursos Afectados

- Todas las **versiones** de Samba **anteriores a 4.13.17.**

Cabe destacar que para que esta vulnerabilidad sea explotable, es necesario que el módulo vfs_fruit se encuentre activo. Para ello se puede lanzar el siguiente comando, el cual, muestra detalles sobre el módulo deseado, incluyendo una descripción, una lista de todos los perfiles y una lista de todos los paquetes proporcionados:

```
$ yum module info vfs_fruit
```

Recomendaciones Actualizadas (03/02/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones recomienda encarecidamente aplicar los siguientes pasos:

Mitigación

1º. Solución a la vulnerabilidad:

Será necesario actualizar lo antes posible a las versiones parcheadas que ha ya ha publicado Samba y que se muestran a continuación:

- Samba 4.14.12.
- Samba 4.15.5.

2º. Workaround de la vulnerabilidad:

Desde la USTIC se recomienda encarecidamente aplicar los parches de seguridad disponibles, con el fin de evitar la exposición a ataques externos y la toma de control de los sistemas informáticos.

En caso de no ser posible aplicar las actualizaciones descritas, el fabricante recomienda eliminar el módulo *VFS_fruit* de la lista de objetos VFS configurados en Samba. Sin embargo, tal y como señala el equipo de Samba, al cambiar la configuración del módulo VSF fruit toda la información asociada al módulo quedará inaccesible, por lo que dispositivos con MacOs no podrán acceder a ella.

Para desactivar un módulo es necesario lanzar el comando mostrado a continuación:

```
$ yum module disable vfs_fruit
```

Por último, es necesario recargar la configuración de Samba para que las modificaciones efectuadas surjan efecto:

```
$ smbcontrol all reload-config
```

En caso de haber detectado la explotación de esta vulnerabilidad :

debe reportar el incidente mediante correo electrónico a sau.cges.sspa@juntadeandalucia.es indicando en el *Asunto: [Compromiso Samba_fruit]*

Para cualquier otra duda o consulta al respecto, puede ponerse en contacto con ustic.stic.sspa@juntadeandalucia.es. **Les seguiremos informando.**

Gracias por su atención.

Unidad de Seguridad TIC

Subdirección de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud