Nro. Alerta:	EC-2022-020	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	4-febrero-2022	**SAMBA: vulnerabilidad permite a atacantes remotos ejecutar código arbitrario como root en Instalaciones que usan el módulo VFS vfs_fruit**	V 1.0

I. DATOS GENERALES:

Clase de alerta: Inyección de Código

Tipo de incidente: Sistema vulnerable

Nivel de riesgo: Medio

II. ALERTA

Samba ha emitido actualizaciones de software para abordar múltiples vulnerabilidades de seguridad que, si se explotan con éxito, podrían permitir a atacantes remotos ejecutar código arbitrario con los privilegios más altos en las instalaciones afectadas.

Figura 1. Logo Sistema Samba **Fuente:** The Hacker News

III. INTRODUCCIÓN

Todas las versiones de Samba anteriores a la 4.13.17, son susceptibles a una vulnerabilidad de lectura y escritura de “montón fuera de límites” (out-of-bounds heap), la cual permite a atacantes remotos, ejecutar código arbitrario como root en las instalaciones de Samba afectadas que usan el módulo VFS vfs_fruit.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-020	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	4-febrero-2022	**SAMBA: vulnerabilidad permite a atacantes remotos ejecutar código arbitrario como root en Instalaciones que usan el módulo VFS vfs_fruit**	V 1.0

Samba es una popular implementación gratuita del protocolo Server Message Block (SMB) que permite a los usuarios acceder a archivos, impresoras y otros recursos comúnmente compartidos a través de una red.

IV. VECTOR DE ATAQUE

Remoto, sistema vulnerable

V. IMPACTO

La falla en el sistema Samba, codificada como CVE-2021-44142, afecta a las distribuciones de Linux ampliamente utilizadas, como Red Hat, SUSE Linux y Ubuntu.

La falla específica, existe en el análisis de metadatos en el demonio del servidor Samba (smbd). Para aprovechar esta vulnerabilidad, se requiere acceso como usuario con acceso de escritura, a los atributos extendidos de un archivo. Se debe tener en cuenta que podría ser un invitado, o un usuario no autenticado si dichos usuarios tienen acceso de escritura a los atributos extendidos del archivo.

El problema en vfs_fruit existe en la configuración predeterminada del módulo fruit VFS usando fruit:metadata=netatalk o fruit:resource=file. Si ambas opciones se establecen en configuraciones diferentes a los valores predeterminados,el sistema no se ve afectado por el problema de seguridad.

VI. RECOMENDACIONES

El EcuCERT, recomienda a su comunidad objetivo, tomar en consideración lo siguiente:

- Mantener actualizado el sistema Samba, aplicando las últimas actualizaciones y parches de seguridad disponibles desde https://www.samba.org/samba/security/, se han emitido las actualizaciones Samba 4.13.17, 4.14.12 y 4.15.5 como versiones de seguridad para corregir la vulnerabilidad CVE-2021-44142.
- Monitorear la infraestructura de red a nivel interno y externo, a través de plataformas de seguridad perimetral, para identificar posible tráfico de carácter anómalo.
- Eliminar el módulo vfs_fruit de la lista de objetos VFS configurados en cualquier línea

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-020	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	4-febrero-2022	**SAMBA: vulnerabilidad permite a atacantes remotos ejecutar código arbitrario como root en Instalaciones que usan el módulo VFS vfs_fruit**	V 1.0

"objetos vfs" en la configuración de Samba smb.conf.
Tener en cuenta que, al cambiar la configuración del módulo VFS fruit:metadata o fruit:resource, para usar la configuración no afectada, hará que toda la información almacenada sea inaccesible, y, hará parecer que la información se ha perdido para los usuarios de macOS.

- Identificar y suspender el acceso de usuarios que exhiban una actividad inusual.
- Implementar un plan de respuesta a emergencias en la Organización/Institución, considerar la gama completa de impactos potenciales que los ciberataques plantean a las operaciones, incluida la pérdida o manipulación de la información, la pérdida o manipulación del control y, las amenazas a la seguridad.
- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

VII. REFERENCIAS:

Samba ORG. (31 de enero de 2022). Samba ORG. Obtenido de https://www.samba.org/samba/security/CVE-2021-44142.html

Ravie Lakshmanán. (31 de enero de 2022). TheHackerNews. Obtenido de https://thehackernews.com/2022/01/new-samba-bug-allows-remote-attackers.html