USTIC-AV 22/22. Disponibles actualizaciones de seguridad para abordar múltiples vulnerabilidades críticas en Samba (21/12/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones **avisa** del lanzamiento de **actualizaciones para** abordar múltiples **vulnerabilidades críticas en Samba** que pueden explotarse para tomar el control de los sistemas afectados.

Detalle

Samba ha lanzado el pasado 15 de diciembre actualizaciones de software para remediar múltiples vulnerabilidades críticas, rastreadas como CVE-2022-38023, CVE-2022-37966, CVE-2022-37967 y CVE-2022-45141 que, si se explotan con éxito, podrían permitir que un atacante tome el control de los sistemas afectados.

A continuación, se incluye una breve descripción de cada una de ellas:

- CVE-2022-38023(puntuación CVSS: 9,8): La más grave de todas. La protección “RC4” del canal NetLogon Secure utiliza los mismos algoritmos que la criptografía RC4-HMAC en Kerberos, por lo que también se debe suponer que es débil.
- CVE-2022-37966(CVSS: 8.1): Elevación de privilegios en Windows Kerberos RC4-HMAC.
- CVE-2022-37967(CVSS: 7.2): Al igual que la anterior, elevación de privilegios en Windows Kerberos.
- CVE-2022-45141(CVSS: 8,1): Los DC de Active Directory de Samba vulnerables emitirán tickets cifrados rc4-hmac a pesar de que el servidor de destino admita un mejor cifrado (p. ej., aes256-cts-hmac-sha1-96).

Según hemos corroborado con los medios de detección disponibles, **estas vulnerabilidades se encuentran presentes en un número de sistemas muy elevado en nuestra organización**, por lo que, debido al riesgo potencial que presentan, llamamos vuestra atención sobre la urgencia de aplicar las recomendaciones indicadas y la adopción de medidas tan pronto como sea posible.

Recursos Afectados

- Todas las versiones de Samba anteriores a 4.15.13, 4.16.8 y 4.17.4.

Recomendaciones Actualizadas (21/12/2022)

La Unidad de Seguridad TIC de la Subdirección de Tecnologías de la Información y Comunicaciones recomienda encarecidamente aplicar los siguientes pasos, con el fin de evitar la exposición a ataques externos y la toma de control de los sistemas informáticos:

Mitigación

1º. Solución a las vulnerabilidades:

Será necesario **actualizar** las versiones afectadas lo antes posible, tal como se muestra a continuación:

- Si utiliza la versión 4.15, actualice a versión 4.15.13
- Si utiliza la versión 4.16, actualice a versión 4.16.8
- Si utiliza la versión 4.17, actualice a versión 4.17.4

Si no pueden actualizar, algunos de los errores mencionados anteriormente pueden mitigarse con cambios de configuración, aunque algunos de ellos desactivan funciones de las que podría depender la red, lo que impediría utilizar esas soluciones concretas.

2º. *Workaround* a las vulnerabilidades:

En los siguientes enlaces, puede encontrarse el *workaround* específico para cada vulnerabilidad:

- CVE-2022-38023: https://www.samba.org/samba/security/CVE-2022-38023.html
- CVE-2022-37966: https://www.samba.org/samba/security/CVE-2022-37966.html
- CVE-2022-37967: https://www.samba.org/samba/security/CVE-2022-37967.html
- CVE-2022-45141: https://www.samba.org/samba/security/CVE-2022-45141.html

Referencias

- Anuncio de Samba
- Detalle de las vulnerabilidades y parches

Para cualquier duda o consulta al respecto, puede ponerse en contacto con nuestro equipo en ustic.stic.sspa@juntadeandalucia.es.

Gracias por vuestra atención.

Unidad de Seguridad TIC

Subdirección de Tecnologías de la Información y Comunicaciones

Servicio Andaluz de Salud