Basque CyberSecurity Centre

Vulnerabilidad de alta severidad en Samba

BCSC-AVISOS

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

TABLA DE CONTENIDO

Sobre el BCSC 3
1. Aviso de seguridad 4
2. Recursos afectados 5
3. Análisis técnico 6
4. Mitigación / Solución 7
5. Referencias Adicionales 8

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

Sobre el BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Aviso de seguridad

Samba ha publicado un aviso de seguridad donde se aborda una vulnerabilidad de severidad alta cuyo identificador es CVE-2023-0614 y que ha sido encontrada en todas las versiones del software Samba desde la versión 4.0.

La vulnerabilidad ya había sido reportada previamente para las versiones de Samba 4.6.16, 4.7.9, 4.8.4 y 4.9.7 habiendo sido registrada con el identificador CVE-2018-10919 y considerada corregida, pero dicha corrección ha resultado ser insuficiente, de forma que, el error sigue pudiendo permitir que un atacante obtenga claves de recuperación confidenciales de BitLocker de un controlador de dominio Active Directory (AD) de Samba. La explotación exitosa de esta vulnerabilidad representa un alto impacto en la confidencialidad de los sistemas afectados.

El fabricante ya ha publicado la actualización correspondiente corrigiendo de esta manera el fallo destacado, por lo que, para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible.

2. Recursos afectados

- Todas las versiones del software Samba de la versión 4.0 en adelante.

3. Análisis técnico

CVE-2023-0614: vulnerabilidad que permite que un atacante obtenga claves de recuperación de BitLocker confidenciales a través de LDAP en todas las versiones de Samba a partir de la 4.0. La vulnerabilidad existe debido a un parche insuficiente para la vulnerabilidad CVE-2018-10919, de manera que, un usuario remoto puede eludir las restricciones de seguridad implementadas y obtener acceso a información confidencial.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.7

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**
- **Integridad:** Ninguna
- **Disponibilidad:** Ninguna

4. Mitigación / Solución

Para la mitigación de estas vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible en cuanto se publiquen las actualizaciones correspondientes.

Para tratar la vulnerabilidad descrita, Samba ha publicado una actualización de seguridad disponible desde:

- https://www.samba.org/samba/history/security.html

También se ha facilitado, dentro del propio aviso, una lista de atributos impactados por la vulnerabilidad.

Adicionalmente, se recomienda a los usuarios de Samba actualizar su software y tomar medidas para asegurarse de que los datos que pudieran haber sido filtrados, desde los atributos confidenciales, ya no sean útiles. Esto puede incluir la reencriptación de unidades encriptadas con BitLocker, cambiar las contraseñas TPM y revocar y reemitir certificados que se almacenan con Credential Roaming (con nuevas claves secretas).

Por último, se han emitido versiones de seguridad de Samba *$VERSIONS* para corregir el problema. Se recomienda a los administradores de Samba que actualicen a estas versiones o apliquen el parche lo antes posible.

5. Referencias Adicionales

- Aviso de seguridad.
- CVE-2023-0614.
- CVE-2018-10919.

EUSKO JAURLARITZA GOBIERNO VASCO
GRUPO spri TALDEA