BOLETÍN DE ALERTA

Boletín Nro.: 2022-32
Fecha de publicación: 01/08/2022
Tema: Vulnerabilidades críticas en productos Samba

Productos afectados:

Todas las versiones anteriores a 4.14.14 de Samba.

Descripción:

Samba ha lanzado actualizaciones de seguridad para subsanar vulnerabilidades en múltiples versiones, que permitirían a un atacante remoto realizar escalamiento de privilegios, denegación de servicios (DoS), entre otros.

- CVE-2022-32744 de severidad alta, con puntuación asignada de 8.8. La vulnerabilidad se debe a fallas en el servicio *KDC kpasswd,* el cual maneja las solicitudes de cambio de contraseña. Esto permitiría a un atacante remoto realizar cambios de contraseñas a los usuarios, incluyendo la del administrador y robar información privilegiada en el sistema. La vulnerabilidad trata de una falla en el restablecimiento de contraseña de administrador (Reset Password) que se puede explotar cifrando solicitudes kpasswd falsificadas con la clave de un usuario normal del sistema, entonces un usuario normal puede cambiar las contraseñas de otros usuarios incluyendo la del administrador, esto permite la toma de control total del dominio.

- CVE-2022-2031 de severidad media, con puntuación asignada de 5.4. La vulnerabilidad se debe a fallas en el servicio *KDC kpasswd,* el cual maneja las solicitudes de cambio de contraseña. Esto permitiría a un atacante remoto realizar escalamiento de privilegios en el sistema.

- CVE-2022-32745 de severidad media, con puntuación asignada de 5.4. Esta vulnerabilidad se debe a un error de limitación en el parámetro 'count' de la memcpy(). Un atacante podría enviar un mensaje especialmente diseñado y poner en peligro la confidencialidad del sistema afectado.

- CVE-2022-32746 de severidad media, con puntuación asignada de 5.4. Esta vulnerabilidad se debe a un error existente en la función realloc() de la base de datos. Esto permitiría a un atacante remoto obtener información sensible de la memoria del sistema.

- CVE-2022-32742 de severidad media, con puntuación asignada de 4.3. Esta vulnerabilidad se debe a fallas en solicitudes SMBv1. Esto permitiría a un atacante remoto obtener información sensible de la memoria del sistema.

Impacto:

La explotación exitosa de estas vulnerabilidades permitiría a un atacante remoto realizar cambios de contraseñas a los usuarios, robar información privilegiada en el sistema y escalamiento de privilegios, así como posible denegación de servicio (DoS).

Mitigación:

Samba ha parchado las vulnerabilidades en sus nuevas versiones 4.16.4, 4.15.9 y 4.14.14. Recomendamos a aquellos que usan una versión vulnerable, instalar el parche lo antes posible, accediendo al siguiente enlace:

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

Información adicional:

- https://www.cert.gov.py/noticias/actualizaciones-de-seguridad-en-samba/
- https://securityonline.info/cve-2022-32744-critical-samba-admin-password-reset-flaw/
- https://www.samba.org/samba/security/CVE-2022-32744.html
- https://www.samba.org/samba/security/CVE-2022-32746.html
- https://www.samba.org/samba/security/CVE-2022-32745.html
- https://www.samba.org/samba/security/CVE-2022-32744.html
- https://www.samba.org/samba/security/CVE-2022-32742.html
- https://www.samba.org/samba/security/CVE-2022-2031.html
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2031
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32742
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32744
- https://www.samba.org/samba/history/security.html