Boletín de alerta

Boletín Nro.:
Fecha de publicación: 16/10/2025
Tema: Alerta 2025-86 Vulnerabilidad critica Samba
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- **Samba** versiones **4.0 y posteriores.**
- Afecta únicamente a **controladores de dominio (AD DC)** con el **servidor WINS habilitado** y el parámetro **wins hook** configurado.

Descripción

Se ha identificado una **vulnerabilidad crítica de ejecución remota de código (RCE)** en Samba, rastreada como **CVE-2025-10230**, que permite a un atacante no autenticado ejecutar comandos arbitrarios en el sistema.

El fallo ocurre cuando el parámetro **wins hook** está activo junto con el soporte **WINS**, permitiendo que datos manipulados se interpreten directamente como comandos del sistema operativo.

Esta vulnerabilidad recibe una **puntuación CVSS de 10.0 (Crítica)** debido a que permite la ejecución remota sin autenticación, comprometiendo completamente la confidencialidad, integridad y disponibilidad del sistema afectado.

Cuando Samba actúa como **controlador de dominio de Active Directory** y tiene habilitado el soporte **WINS**, el parámetro **wins hook** ejecuta un script cada vez que se cambia un nombre WINS.

El problema radica en que **no se valida adecuadamente el contenido del nombre WINS**, lo que permite la inserción de **entradas que permiten inyección directa en la línea de comandos del sistema** dentro del comando ejecutado.

Un atacante remoto puede enviar solicitudes WINS especialmente diseñadas para inyectar comandos maliciosos y ejecutar código con los privilegios del servicio Samba.

Solución:

Actualizar Samba a una versión segura:

- **4.23.2**, **4.22.5** o **4.21.9**, disponibles en

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

Desactivar temporalmente el parámetro vulnerable si no es posible actualizar:

- En el archivo smb.conf, asegúrese de que:

wins support = no

- o que el parámetro esté vacío:

wins hook =

Esta configuración evita la ejecución del script vulnerable.

Información adicional:

https://www.samba.org/samba/security/CVE-2025-10230.html

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