Servicio De Samba Es Atacado Por Vulnerabilidad De Código

Una vulnerabilidad crítica se ha solucionado en Samba, el estándar Open Source para la interoperabilidad de programas Windows para Linux y Unix, que podría haber permitido a los hackers ejecutar remotamente un código arbitrario en el **proceso demonio Samba** (smbd).

Samba es una implementación de código abierto del protocolo de uso compartido de archivos de red SMB/CIFS, funciona en la mayoría de los sistemas operativos disponibles en la actualidad, lo que permite a un servidor que no sea Windows comunicarse con el mismo protocolo de red con las aplicaciones de Windows. Samba es soportado por muchos sistemas operativos, incluyendo Windows 95/98 / NT, OS / 2 y Linux.

La vulnerabilidad, llamada como **CVE-2015-0240**, en realidad reside en el demonio del servidor de archivos smbd. El error puede ser usado por los hackers para **ejecutar código remoto con privilegios de root**, segun ha advertido el equipo de desarrollo de Samba.

El equipo descubrió que la vulnerabilidad permite a un cliente malicioso enviar algunos paquetes que podrían liberar memoria en un paquete de sesión anónimo, lo que lleva a la ejecución de código inesperado al azar. En el caso, **se requieren privilegios de root**, lo cual es automático y no de inicio de sesión o la autenticación es necesaria.

La vulnerabilidad de la seguridad afecta a todas las versiones del software Samba, desde la versión estable más antigua soportada, hasta las versiones de Samba 3.5.0, en la versión de desarrollo actual, 4.2.0 Release Candidate (RC) 4.

Equipo de productos de Red Hat publicó un análisis detallado de esta vulnerabilidad en su blog. Según los investigadores, las versiones de Red Hat Enterprise Linux 5 a 7 se ven afectadas, al igual que las versiones de Red Hat Storage Server 2.1 y 3. Salvo RHEL7, la vulnerabilidad se considera crítica para todos los productos afectados. Otras distribuciones de Linux también han publicado alertas de seguridad acerca de la vulnerabilidad.

Mientras tanto, otras distribuciones de Linux más importantes, incluyendo **Ubuntu**, Debian y Suse, también han lanzado una actualización de paquetes en sus repositorios, con otros que pronto serán lanzados.