La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), agregó el jueves una vulnerabilidad de alta gravedad recientemente revelada en la suite de correo electrónico Zimbra a su Catálogo de Vulnerabilidades Explotadas Conocidas, citando evidencia de explotación activa.

La vulnerabilidad se rastrea como CVE-2022-27924 (puntuación CVSS: 7.5), y es una falla de inyección de comandos en la plataforma que podría conducir a la ejecución de comandos arbitrarios de Memcached y al robo de información confidencial.

> *«Zimbra Collaboration (ZCS) permite que un atacante inyecte comandos memcached en una instancia específica, lo que provoca una sobrescritura de entradas arbitrarias en caché»,* dijo CISA.

Específicamente, el error se relaciona con un caso de validación insuficiente de la entrada del usuario que, de ser explotada exitosamente, podría permitir a los atacantes robar credenciales de texto sin formato de los usuarios de las instancias de Zimbra específicas.

El problema fue revelado por SonarSource en junio, con parches lanzados por Zimbra el 10 de mayo de 2022, en las versiones 8.8.15P31.1 y 9.0.0P21.4.

CISA no compartió los detalles técnicos de los ataques cibernéticos que explotan la vulnerabilidad en la naturaleza, y aún tiene que atribuirla a un determinado actor de amenazas.

A la luz de la explotación activa de la falla, se recomienda a los usuarios que apliquen las actualizaciones al software para reducir su exposición a posibles ataques cibernéticos.