Se está explotando activamente una grave vulnerabilidad de ejecución remota de código en el software de colaboración empresarial y la plataforma de correo electrónico de Zimbra, y actualmente no existen parches disponibles para corregir el problema.

La vulnerabilidad, rastreada como CVE-2022-41352, tiene una calificación de gravedad crítica de 9.8, lo que proporciona una vía para que los atacantes carguen archivos arbitrarios y realicen acciones maliciosas en las instalaciones afectadas.

> *«La vulnerabilidad se debe al método (cpio) en el que el motor antivirus de Zimbra (Amavis) escanea los correos electrónicos entrantes»,* dijo la compañía de seguridad cibernética Rapid7.

Se cree que se ha abusado del problema desde inicios de septiembre de 2022, según los detalles compartidos en los foros de Zimbra. Aunque aún no se ha lanzado una solución, Zimbra insta a los usuarios a instalar la utilidad «pax» y reiniciar los servicios de Zimbra.

> *«Si el paquete pax no está instalado, Amavis recurrirá al uso de cpio, desafortunadamente, el respaldo está mal implementado (por Amavis) y permitirá que un atacante no autenticado cree y sobrescriba archivos en el servidor Zimbra, incluyendo el webroot de Zimbra»,* dijo la compañía el mes pasado.

La vulnerabilidad, que está presente en las versiones 8.8.15 y 9.0 del software, afecta a varias distribuciones de Linux como Oracle Linux 8, Red Hat Enterprise Linux 8, Rocky Linux 8 y CentOS 8, con la excepción de Ubuntu debido a que ese pax ya viene instalado por defecto.

Una explotación exitosa de la vulnerabilidad requiere que un atacante envíe por correo electrónico un archivo de almacenamiento (CPIO o TAR) a un servidor susceptible, que después es inspeccionado por Amavis utilizando la utilidad de archivador de archivos cpio para extraer su contenido.

> *«Debido a que cpio no tiene un modo en el que pueda usarse de forma segura en archivos que no son de confianza, el atacante puede escribir en cualquier ruta del sistema de archivos a la que pueda acceder el usuario de Zimbra. El resultado más probable es que el atacante plante un shell en la raíz web para obtener la ejecución remota del código, aunque es probable que existan otras vías»*, dijo Ron Bowes, investigador de Rapid7.

Zimbra dijo que espera que la vulnerabilidad se aborde en el próximo parche de Zimbra, que eliminará la dependencia de cpio, y en cambio, hará que pax sea un requisito. Sin embargo, no ha ofrecido un marco de tiempo específico sobre cuándo estará disponible la solución.

Rapid7 también dijo que CVE-2022-41352 es *«efectivamente idéntico»* a CVE-2022-30333, una falla transversal en la versión Unix de la utilidad unRAR de RARlab que salió a la luz a inicios de junio, la única diferencia es que la nueva vulnerabilidad aprovecha formatos de archivo CPIO y TAR en lugar de RAR.

Aún más preocupante, se dice que Zimbra es más vulnerable a otra falla de escalada de privilegios de día cero, que podría estar encadenada con el día cero de cpio para lograr un compromiso remoto de raíz de los servidores.

El hecho de que Zimbra haya sido un objetivo popular para los atacantes no es nuevo. En agosto, la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), advirtió sobre los adversarios que explotan múltiples fallas en el software para violar las redes.