Una nueva vulnerabilidad de alta gravedad fue revelada en el paquete de correo electrónico de Zimbra, que de ser explotada exitosamente, permite que un atacante no autenticado robe contraseñas de texto sin cifrar de los usuarios sin ninguna interacción del usuario.

> *«Con el consiguiente acceso a los buzones de correo de las víctimas, los atacantes pueden escalar potencialmente su acceso a organizaciones objetivo y obtener acceso a varios servicios internos y robar información altamente confidencial»,* dijo SonarSource.

Rastreada como CVE-2022-27924, con puntuación CVSS de 7.5, la vulnerabilidad se caracteriza como un caso de *«envenenamiento de Memcached con solicitud no autenticada»*, lo que lleva a un escenario en el que un adversario puede inyectar comandos maliciosos y desviar información confidencial.

Esto es posible gracias al envenenamiento de las entradas de caché de ruta IMAP en el servidor Memcached que se usa para buscar usuarios de Zimbra y reenviar sus solicitudes HTTP a los servicios de back-end apropiados.

Debido a que Memcached analiza las solicitudes entrantes línea por línea, la vulnerabilidad permite que un atacante envíe una solicitud de búsqueda especialmente diseñada al servidor que contiene caracteres CRLF, lo que hace que el servidor ejecute comandos no deseados.

La falla existe porque *«los caracteres de nueva línea (/r/n) no se escapan en la entrada de un usuario que no es de confianza. Esta falla en el código finalmente permite a los atacantes robar credenciales de texto claro de los usuarios de las instancias de Zimbra específicas»*, dijeron los investigadores.

Armado con esta capacidad, el atacante puede posteriormente corromper el caché para sobrescribir una entrada de modo que reenvíe todo el tráfico IMAP a un servidor controlado por el atacante, incluidas las credenciales del usuario objetivo en texto no cifrado.

El ataque presupone que el adversario ya está en posesión de las direcciones de correo electrónico de las víctimas para poder envenenar las entradas del caché y que utilizan un cliente IMAP para recuperar mensajes de correo electrónico de un servidor de correo.

> *«Por lo general, una organización usa un patrón para las direcciones de correo electrónico de sus miembros, como por ejemplo {nombre}.{apellido}@example.com. Se puede obtener una lista de direcciones de correo electrónico de fuentes OSINT como LinkedIn»*, dijeron los investigadores.

Sin embargo, un atacante puede eludir estas restricciones al explotar una técnica llamada contrabando de respuestas, que implica el *«contrabando»* de respuestas HTTP no autorizadas que abusan de la falla de inyección CRLF para reenviar el tráfico IMAP a un servidor no autorizado, robando así las credenciales de direcciones de correo electrónico de los usuarios sin conocimiento previo.

> *«La idea es que al inyectar continuamente más respuestas que elementos de trabajo en los flujos de respuesta compartidos de Memcached, podemos forzar búsquedas aleatorias de Memcached para usar respuestas inyectadas en lugar de la respuesta correcta. Esto funciona porque Zimbra no validó la clave de la respuesta de Memcached al consumirla»,* agregaron los investigadores.

Después de la divulgación responsable el 11 de marzo de 2022, Zimbra envió parches para corregir completamente la vulnerabilidad el 10 de mayo de 2022, en las versiones 8.8.15 P31.1 y 9.0.0 P24.1.