BOLETÍN DE ALERTA

Boletín Nro.: 2022-26
Fecha de publicación: 16/06/2022
Tema: Vulnerabilidad crítica en Zimbra

La vulnerabilidad está presente en las versiones anteriores a:

- Zimbra Collaboration Kepler 9.0.0 Parche 24.1
- Zimbra Collaboration Joule 8.8.15 Parche 31.1

Descripción:

Se ha reportado una nueva vulnerabilidad en el servidor de correo electrónico Zimbra, que permitiría a un atacante no autenticado robar contraseñas de acceso sin cifrar de los usuarios sin ninguna interacción del usuario y realizar ejecución remota de código (RCE).

La vulnerabilidad identificada como CVE-2022-27924 de severidad alta, con puntuación asignada de 7.5. Esta se debe a la falla del componente Memcached del servidor Zimbra, Memcached es un sistema de almacenamiento de clave-valor en memoria para usar como caché de alto rendimiento o almacenamiento de sesiones para bases de datos externas y llamadas API, en este caso el servicio de búsqueda.

La vulnerabilidad se explota a través del 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.

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría a un atacante no autenticado robar contraseñas de acceso y realizar ejecución remota de código (RCE) en una instancia de destino.

Métodos de ataques:

Las estrategias que podrían ser utilizadas por los atacantes para explotarla son:

1. **Conocer** la dirección de correo electrónico de las víctimas y aguardar que utilicen un cliente IMAP, para lograr robar sus credenciales de inicio de sesión.

2. **Utilizar** *Response Smuggling* para prescindir de los requerimientos de la primera estrategia y permitir al atacante robar credenciales de texto sin cifrar, de cualquier instancia vulnerable de Zimbra sin necesidad de conocer el correo electrónico específico

Mitigación:

Zimbra parchó la vulnerabilidad creando un hash SHA-256 de todas las claves de Memcache antes de enviarlas al servidor de Memcache. Como la representación de cadena hexadecimal de un SHA-256 no puede contener espacios en blanco, ya no se pueden inyectar líneas nuevas. Las versiones corregidas son respectivamente 8.8.15 con nivel de parche 31.1 y 9.0.0 con nivel de parche 24.1.

Recomendamos actualizar con los siguientes enlaces proporcionados por Zimbra:

- https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P31.1
- https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P24.1

Información adicional:

- https://cert.gov.py/noticias/vulnerabilidad-de-rce-en-servidor-de-correo-electronico-zimbra
- https://csirt.telconet.net/comunicacion/noticias-seguridad/vulnerabilidad-zero-day-zimbra-cve-2022-27924-permite-que-los-atacantes-roben-credenciales-de-inicio-de-sesion-sin-autenticacion/
- https://thehackernews.com/2022/06/new-zimbra-email-vulnerability-could.html
- https://nvd.nist.gov/vuln/detail/CVE-2022-27924