BOLETÍN DE ALERTA

Boletín Nro.: 2022-29
Fecha de publicación: 29/06/2022
Tema: Vulnerabilidad de UnRar Path Traversal afecta a Zimbra Mail

La vulnerabilidad está presente en versiones anteriores a:

- UnRar, versión 6.12.

Descripción:

Se ha reportado una vulnerabilidad del tipo *directory traversal* en UnRar de RarLab, que permitiría a un atacante realizar ejecución remota de código (RCE) con el usuario que ejecuta el servicio zimbra en el sistema afectado.

La vulnerabilidad identificada como CVE-2022-30333 de severidad alta y puntuación de 7.5. Esta vulnerabilidad se debe a la extracción realizada por la herramienta UnRar incluida en el servicio Amavisd utilizado por Zimbra, de un archivo creado con fines malintencionados fuera del directorio predeterminado, logrando una escritura de archivos en una ubicación especificada.
La vulnerabilidad, en esencia, se relaciona con un ataque de enlace simbólico en el que se crea un archivo RAR de modo que contenga un enlace simbólico que es una combinación de barras diagonales y barras diagonales inversas (p. ej., **"..\..\..\tmp/ shell"**) para omitir las comprobaciones actuales y extraer el archivo malicioso fuera del directorio esperado.
Específicamente, la falla tiene que ver con una función que está diseñada para convertir barras invertidas ('\') en barras diagonales ('/') para que un archivo RAR creado en Windows pueda extraerse en un sistema Unix, alterando efectivamente el enlace simbólico antes mencionado a **"../../../tmp/shell"**.
Al aprovechar este comportamiento, un atacante puede escribir archivos arbitrarios en cualquier lugar del sistema de archivos de destino, incluida la creación de un shell JSP (Webshell para Java Web) en el directorio web de Zimbra y ejecutar comandos maliciosos.

La explotación combinada de esta vulnerabilidad permitiría al atacante acceder a los correos electrónicos enviados/recibidos en un servidor de correo electrónico comprometido, e incluso iniciar sesión a través de una puerta trasera configurada de manera silenciosa, así como robar las credenciales de los usuarios de correo. El único requisito para realizar el ataque es que UnRar esté instalado en el servidor de correos Zimbra, hecho bastante frecuente, ya que la herramienta se utiliza para el escaneo de adjuntos de correos electrónicos.

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría a un atacante obtener acceso

completo al servidor de correo electrónico.

Solución:

Se recomienda actualizar a la versión 6.12, proveída en el siguiente enlace:

- https://www.rarlab.com/download.htm

Nota: asegurarse de estar utilizando la versión parchada de UnRar. Para los administradores que deseen instalar UnRar a través de un administrador de paquetes, deben verificar si su repositorio contiene la versión parchada, ya que las versiones pueden diferir según la distribución de Linux que utilicen.

Información adicional:

- https://twitter.com/scannell_simon/status/1541800107909185537?s=21&t=E9KCndendM2len1AB-0erw
- https://blog.sonarsource.com/zimbra-pre-auth-rce-via-unrar-0day/
- https://nvd.nist.gov/vuln/detail/CVE-2022-30333