Investigadores en ciberseguridad han revelado detalles de vulnerabilidades en el software de correo web Roundcube que podrían ser explotadas para ejecutar JavaScript malicioso en el navegador web de una víctima y robar información sensible de su cuenta bajo ciertas condiciones.

> *«Cuando una víctima abre un correo electrónico malicioso en Roundcube enviado por un atacante, este puede ejecutar JavaScript arbitrario en el navegador de la víctima»,* afirmó la compañía de ciberseguridad Sonar en un análisis publicado esta semana.
>
> *«Los atacantes pueden aprovechar la vulnerabilidad para robar correos electrónicos, contactos y la contraseña del correo de la víctima, además de enviar correos electrónicos desde la cuenta de la víctima.»*

Tras la divulgación responsable el 18 de junio de 2024, las tres vulnerabilidades se han solucionado en las versiones 1.6.8 y 1.5.8 de Roundcube, lanzadas el 4 de agosto de 2024.

La lista de vulnerabilidades es la siguiente:

- CVE-2024-42008: Un fallo de cross-site scripting a través de un adjunto de correo electrónico malicioso con un encabezado Content-Type peligroso.
- CVE-2024-42009: Un fallo de cross-site scripting que se origina en el postprocesamiento de contenido HTML sanitizado.
- CVE-2024-42010: Un fallo de divulgación de información debido a un filtrado insuficiente de CSS.

La explotación exitosa de las vulnerabilidades mencionadas podría permitir a atacantes no autenticados robar correos electrónicos y contactos, así como enviar correos electrónicos desde la cuenta de una víctima, después de abrir un correo electrónico especialmente diseñado en Roundcube.

> *«Los atacantes pueden establecer una presencia persistente en el navegador de la víctima a través de reinicios, lo que les permite exfiltrar correos electrónicos continuamente o robar la contraseña de la víctima la próxima vez que se ingrese»*, dijo el investigador de seguridad Oskar Zeino-Mahmalat.

> *«Para que el ataque sea exitoso, no se requiere interacción del usuario más allá de abrir el correo electrónico del atacante para explotar la vulnerabilidad crítica de XSS (CVE-2024-42009). Para CVE-2024-42008, se necesita un solo clic de la víctima para que el exploit funcione, pero el atacante puede hacer que esta interacción no sea obvia para el usuario.»*

Se han retenido detalles técnicos adicionales sobre los problemas para dar tiempo a los usuarios de actualizar a la última versión, y considerando que las vulnerabilidades en el software de correo web han sido explotadas repetidamente por actores estatales como APT28, Winter Vivern y TAG-70.

Los hallazgos surgen mientras se han revelado detalles sobre una vulnerabilidad de escalada de privilegios locales de máxima severidad en el proyecto de código abierto RaspAP (CVE-2024-41637, puntuación CVSS: 10.0) que permite a un atacante elevar sus privilegios a root y ejecutar varios comandos críticos. La vulnerabilidad ha sido solucionada en la versión 3.1.5.

> *«El usuario www-data tiene permisos de escritura en el archivo restapi.service y también posee privilegios de sudo para ejecutar varios comandos críticos sin una contraseña. Esta combinación de permisos permite a un atacante modificar el servicio para ejecutar código arbitrario con privilegios de root, escalando su acceso de www-data a root»*, dijo un investigador de seguridad conocido como 0xZon1.