El individuo amenazante identificado como Vivern Winter ha sido observado aprovechando una vulnerabilidad de día cero en el software de correo web Roundcube el 11 de octubre de 2023, con el propósito de recolectar mensajes de correo electrónico de las cuentas de las víctimas.

«Invierno Vivern ha intensificado sus operaciones al hacer uso de una vulnerabilidad previamente desconocida en Roundcube», señaló Matthieu Faou, investigador de seguridad de ESET, en un nuevo informe publicado hoy. Previamente, se servía de vulnerabilidades conocidas en Roundcube y Zimbra, para las cuales se pueden encontrar ejemplos prácticos en línea.

Invierno Vivern, también conocido como TA473 y UAC-0114, es un conjunto adversario cuyos objetivos concuerdan con los de Bielorrusia y Rusia. En los últimos meses, se le ha atribuido a ataques contra Ucrania y Polonia, además de contra organismos gubernamentales en Europa e India.

Se ha evaluado que el grupo ha aprovechado una vulnerabilidad previa en Roundcube (CVE-2020-35730), convirtiéndose en el segundo conjunto estatal después de APT28 en atacar el software de correo web de código abierto.

La nueva vulnerabilidad de seguridad en cuestión es CVE-2023-5631 (puntuación CVSS: 5.4), una vulnerabilidad de secuencias de comandos almacenadas que podría permitir a un atacante remoto cargar código JavaScript arbitrario. Se lanzó una solución el 14 de octubre de 2023.

Las cadenas de ataque desplegadas por el conjunto comienzan con un mensaje de suplantación de identidad que incorpora una carga codificada en Base64 en el código fuente HTML y que, a su vez, descodifica una inyección de JavaScript desde un servidor remoto al aprovechar la vulnerabilidad de la inyección de código.

> *«En resumen, al enviar un mensaje de correo electrónico especialmente diseñado,*

> *los atacantes pueden cargar código JavaScript arbitrario en el contexto de la ventana del navegador del usuario de Roundcube. No se requiere ninguna interacción manual aparte de ver el mensaje en un navegador web»*, explicó Faou.

La segunda etapa del JavaScript (checkupdate.js) actúa como un cargador que facilita la ejecución de una carga final de JavaScript que permite al individuo amenazante extraer mensajes de correo electrónico hacia un servidor de control y comando (C2).

> *«A pesar de la limitada complejidad de las herramientas empleadas por el conjunto, representa una amenaza para los gobiernos en Europa debido a su persistencia, la ejecución constante de campañas de suplantación de identidad y a que un número considerable de aplicaciones accesibles desde Internet no se actualizan regularmente, a pesar de que se sabe que contienen vulnerabilidades»,* indicó Faou.