Se reveló una vulnerabilidad de seguridad de alta gravedad sin parchear en el cliente de correo electrónico basado en la web Rain Loop de código abierto, que podría usarse como arma para desviar correos electrónicos de las bandejas de entrada de las víctimas.

> *«La vulnerabilidad del código puede ser explotada fácilmente por un atacante enviando un correo electrónico malicioso a una víctima que usa RainLoop como cliente de correo»,* dijo Simon Scannell, investigador de seguridad de SonarSource.

> *«Cuando la víctima ve el correo electrónico, el atacante obtiene control total sobre la sesión de la víctima y puede robar cualquiera de sus correos electrónico, incluidos aquellos que contienen información altamente confidencial, como contraseñas, documentos y enlaces de restablecimiento de contraseña».*

Rastreada como CVE-2022-29360, la falla se relaciona con una vulnerabilidad de secuencias de comandos entre sitios (XSS) almacenada, que afecta a la última versión de RainLoop v1.16.0 que se lanzó el 7 de mayo de 2021.

Las vulnerabilidades XSS almacenadas, también llamadas XSS persistentes, ocurren cuando un script malicioso se inyecta directamente en el servidor de una aplicación web de destino mediante la entrada del usuario (por ejemplo, un campo de comentarios) que se almacena permanentemente en una base de datos y luego se entrega a otros usuarios.

Al impactar todas las instalaciones de RainLoop que se ejecutan con configuraciones predeterminadas, las cadenas de ataque que aprovechan la falla podrían tomar la forma de un correo electrónico especialmente diseñado enviando a víctimas potenciales que, cuando se ven, ejecuta una carga útil de JavaScript malicioso en el navegador sin requerir ninguna interacción del usuario.

SonarSource, en su cronograma de divulgación, dijo que notificó a los mantenedores de

RainLoop sobre el error el 30 de noviembre de 2021, y que el fabricante de software no ha podido solucionarlo durante más de 4 meses.

Debido a que no hay parches, SonarSource recomienda a los usuarios que migren a una bifurcación RainLoop llamada SnappyMail, que se mantiene activamente y no se ve afectada por la vulnerabilidad de seguridad.