Se ha encontrado una vulnerabilidad de seguridad en el lenguaje de programación R que podría ser aprovechada por un agente malintencionado para crear un archivo RDS (R Data Serialization) malicioso, lo que resultaría en la ejecución de código al cargarlo y hacer referencia a él.

La falla, identificada con el CVE CVE-2024-27322 (puntuación CVSS: 8.8), *«implica el uso de objetos de promesa y evaluación diferida en R,»* según un informe de la compañía de seguridad de aplicaciones de inteligencia artificial HiddenLayer.

Al igual que pickle en Python, RDS es un formato utilizado para serializar y guardar el estado de estructuras de datos u objetos en R, un lenguaje de programación de código abierto utilizado en cálculos estadísticos, visualización de datos y aprendizaje automático.

Este proceso de serialización -serialize() o saveRDS() – y deserialización – unserialize() y readRDS() – también se utiliza al guardar y cargar paquetes R.

La causa principal detrás de CVE-2024-27322 radica en que podría conducir a la ejecución de código arbitrario al deserializar datos no confiables, dejando así a los usuarios expuestos a ataques de la cadena de suministro mediante paquetes R especialmente diseñados.

Un atacante que busque aprovechar esta falla podría aprovechar el hecho de que los paquetes R utilizan el formato RDS para guardar y cargar datos, provocando la ejecución automática de código cuando se descomprime y deserializa el paquete.

> *«Los paquetes R son vulnerables a este exploit y, por lo tanto, pueden ser utilizados como parte de un ataque de la cadena de suministro a través de repositorios de paquetes. Para que un atacante tome el control de un paquete R, todo lo que necesita hacer es sobrescribir el archivo rdx con el archivo manipulado maliciosamente, y cuando se cargue el paquete, se ejecutará automáticamente el código»,* afirmaron los investigadores de seguridad Kasimir Schulz y Kieran Evans.

La falla de seguridad ha sido resuelta en la versión 4.4.0 lanzada el 24 de abril de 2024, tras una divulgación responsable.

> *«Un atacante puede aprovechar esta [falla] mediante la creación de un archivo en formato RDS que incluya una instrucción promise configurando el valor en unbound_value y la expresión para contener código arbitrario. Debido a la evaluación perezosa, la expresión solo se evaluará y ejecutará cuando se acceda al símbolo asociado con el archivo RDS»*, explicó HiddenLayer.
>
> *«Por lo tanto, si se trata simplemente de un archivo RDS, cuando un usuario le asigne un símbolo (variable) para trabajar con él, el código arbitrario se ejecutará al hacer referencia a ese símbolo. Si el objeto está integrado en un paquete R, dicho paquete puede ser agregado a un repositorio R como CRAN, y la expresión será evaluada y se ejecutará el código arbitrario cuando un usuario cargue dicho paquete.»*

Actualización

El Centro de Coordinación CERT (CERT/CC) ha emitido un aviso para CVE-2024-27322, indicando que la falla podría ser explotada para lograr la ejecución de código arbitrario en el dispositivo objetivo de la víctima mediante archivos RDS o rdx malintencionados.

> *«Un atacante puede crear archivos .rds y .rdx maliciosos y utilizar la ingeniería social para distribuir esos archivos y ejecutar código arbitrario en el dispositivo de la víctima. Los proyectos que emplean readRDS en archivos no confiables también son susceptibles al ataque»*, informó CERT/CC.