Investigadores de seguridad de RACK911 Labs, dijeron en un informe publicado esta semana, que encontraron vulnerabilidades de *«carrera de enlaces simbólicos»* en 28 de los productos antivirus más populares actualmente.

RACK911 asegura que los errores pueden ser explotados por un atacante para eliminar los archivos utilizados por el antivirus o por el sistema operativo, lo que ocasiona fallas o deja la computadora inutilizable.

La vulnerabilidad en el corazón de estos bugs se denomina *«carrera de enlace simbólico»*, según el Dr. Vesselin Bontchev, miembro del Laboratorio Nacional de Virología del ordenador en la Academia de Ciencias de Bulgaria.

Se produce una vulnerabilidad de carrera de enlace simbólico cuando se vincula un archivo malicioso y un archivo legítimo, y termina ejecutando acciones maliciosas en el archivo legítimo. Las vulnerabilidades de carrera de enlaces simbólicos por lo genera se utilizan para vincular archivos maliciosos a elementos con mayores privilegios, lo que resulta en ataques de elevación de privilegios (EoP).

> *«Es un problema muy real y antiguo con los sistemas operativos que permiten procesos concurrentes. Se ha descubierto que muchos programas sufren en el pasado»,* dijo Bontchev a ZDNet.

En su informe, el equipo de RACK911 dijo que ha estado investigando la presencia de dichos errores en los productos antivirus desde 2018.

Descubrieron que 28 productos para Linux, Mac y Windows son vulnerables, y notificaron a los proveedores a medida que pasaba el tiempo.

> *«La mayoría de los proveedores de antivirus han reparado sus productos con algunas desafortunadas excepciones»*, dijo el equipo de RACK911.

Algunos proveedores reconocieron los problemas en los avisos públicos, mientras que otros parecen haber implementado parches silenciosos. El equipo de RACK911 no nombró los productos que no se han parcheado.

Los investigadores dijeron que los productos antivirus, son particularmente vulnerables a este tipo de ataques, debido a la forma en que funcionan. Existe un intervalo desde el momento en que los archivos se analizan y se consideran maliciosos y hasta que el antivirus interviene para eliminar la amenaza. El ataque se basa en reemplazar el archivo malicioso con un enlace simbólico a un archivo legítimo dentro de esta ventana de tiempo.

Los investigadores crearon scripts de prueba de concepto que abusan de una condición de carrera para vincular archivos maliciosos a archivos legítimos por medio de uniones de directorio (en Windows) y enlaces simbólicos (en Mac y Linux).

Cuando el antivirus detecta el archivo malicioso y se mueve para eliminarlo, termina eliminando sus propios archivos o eliminando los archivos principales que posee el sistema operativo.

> *«En nuestras pruebas en Windows, macOS y Linux, pudimos eliminar fácilmente los archivos importantes relacionados con el software antivirus que lo volvieron ineficaz, e incluso eliminar archivos clave del sistema operativo que causarían una corrupción significativa que requeriría una reinstalación completa del sistema operativo»,* dijo RACK911.

El código de prueba de concepto que RACK911 lanzó esta semana solo elimina archivos. El Dr. Bontchev afirma que dichos ataques serían más peligrosos si los ataques reescribieran archivos, lo que podría ser factible, y conducirían a una toma total del sistema atacado.

Los ataques en el mundo real que utilizan los errores requerirían que un atacante esté en

condiciones de descargar primero y luego ejecutar el código de ataque de enlace simbólico en un dispositivo. Esto no es algo que ayude a los hackers a violar un sistema, sino algo que podría ayudarlos a mejorar su acceso en un sistema ya pirateado.

Esto quiere decir que este tipo de error solo se puede usar como una carga útil de segunda etapa en una infección de malware, para elevar los privilegios, para deshabilitar productos de seguridad o para sabotear computadoras en un ataque destructivo.

> *«No se equivoquen al respecto, explotar estas fallas fue bastante trivial y los autores de malware experimentados no tendrán problemas para utilizar las tácticas descritas en esta publicación de blog»,* dijo el equipo de RACK911.

Mientras tanto, la mayoría de los errores que RACK911 encontró en los productos antivirus fueron reparados. Sin embargo, las variaciones podrían ser fácilmente descubiertas. Los errores de condición de carrera de enlace simbólico han sido algunos de los errores más antiguos y difíciles de mitigar en aplicaciones en las últimas décadas, en todos los sistemas operativos.