Investigadores de seguridad cibernética revelaron este lunes los detalles de las vulnerabilidades de seguridad encontradas en las soluciones populares que podrían permitir a los atacantes elevar sus privilegios, ayudando así al malware a mantener su punto de apoyo en los sistemas comprometidos.

Según un informe publicado hoy por CyberArk Labs, los altos privilegios asociados a menudo con los productos antimalware los hacen más vulnerables a la explotación a través de ataques de manipulación de archivos, lo que da como resultado un escenario en el que el malware obtiene permisos elevados en el sistema.

Los errores impactan en una amplia gama de soluciones antivirus, incluidas las de Kaspersky, McAfee, Symantec, Fortinet, Check Point, Trend Micro, Avira y Microsoft Defender, cada una de las cuales ya fue corregida por su proveedor.

La principal falla es la capacidad de eliminar archivos de ubicaciones arbitrarias, lo que permite al atacante eliminar cualquier archivo en el sistema, así como una vulnerabilidad de corrupción de archivos que permite al atacante eliminar contenido de cualquier archivo en el sistema.

Según CyberArk, los errores son el resultado de las DACL predeterminadas (Listas de Control de Acceso Discrecional) para la carpeta «C:\ProgramData» de Windows, que son las aplicaciones para almacenar datos para usuarios estándar sin necesidad de permisos adicionales.

Debido a que cada usuario tiene permiso de escritura y eliminación en el nivel base del directorio, aumenta la probabilidad de una escalada de privilegios cuando un proceso sin privilegios crea una nueva carpeta en «ProgramData» a la que después podría acceder un proceso con privilegios.

Las vulnerabilidades pueden ser rastreadas para cada antivirus de la siguiente forma:

- Centro de seguridad de Kaspersky: CVE-2020-25043, CVE-2020-25044,

CVE-2020-25045
- McAfee Endpoint Security y McAfee Total Protection: CVE-2020-7250, CVE-2020-7310
- Symantec Norton Power Eraser: CVE-2019-1954
- Fortinet FortiClient: CVE-2020-9290
- Check Point ZoneAlarm y Check Point Endpoint Security: CVE-2019-8452
- Trend Micro HouseCall para redes domésticas: CVE-2019-19688, CVE-2019-19689 y tres fallas más sin asingar
- Avira: CVE-2020-13903
- Microsoft Defender: CVE-2019-1161

En un caso específico, se observó que dos procesos diferentes, uno con privilegios y el otro que se ejecuta como un usuario local autenticado, compartían el mismo archivo de registro, lo que podría permitir a un atacante explotar el proceso con privilegios para eliminar el archivo y crear un enlace simbólico que apunte a cualquier archivo arbitrario deseado con contenido malicioso.

Posteriormente, los investigadores de CyberArk explotaron la posibilidad de crear una nueva carpeta en «C:\ProgramData» antes de que se ejecute un proceso privilegiado.

Al hacer esto, descubrieron que al ejecutar el instalador del antivirus McAfee después de crear la carpeta «McAfee», el usuario estándar tiene el control total sobre el directorio, lo que permite al usuario local obtener permisos elevados mediante la realización de un ataque de enlace simbólico.

Además, un atacante podría haber aprovechado una falla de secuestro de DLL en Trend Micro, Fortinet y otras soluciones antivirus para agregar un archivo DLL malicioso en el directorio de la aplicación y elevar los privilegios.

Al instar que las listas de control de acceso deben ser restrictivas para evitar vulnerabilidades de eliminación arbitrarias, CyberArk enfatizó la necesidad de actualizar los marcos de instalación para mitigar los ataques de secuestro de DLL.

Aunque es posible que se hayan abordado estos problemas, el informe sirve como recordatorio de que las debilidades en el software, incluidas las que tienen como objetivo ofrecer protección antivirus, pueden ser un conducto para el malware.

> *«Las implicaciones de estos errores son a menudo una escalada de privilegios total del sistema local. Debido al alto nivel de privilegios de los productos de seguridad, un error en ellos podría ayudar al malware a mantenerse firme y causar más daño a la organización»*, dijeron los investigadores de CyberArk.