Se emitieron parches no oficiales para corregir una vulnerabilidad de seguridad de Windows parcheada incorrectamente, que podría permitir la divulgación de información y la escalada de privilegios locales (LPE) en sistemas vulnerables.

Rastreada como CVE-2021-24084, con puntuación CVSS de 5.5, la falla se refiere a una vulnerabilidad de divulgación de información en el componente de administración de dispositivos de Windows Mobile, que podría permitir a un atacante obtener acceso no autorizado al sistema de archivos y leer archivos arbitrarios.

Se le atribuyó el descubrimiento e informe del error al investigador de seguridad Abdelhamid Naceri, en octubre de 2020, lo que llevó a Microsoft a abordar el problema como parte de sus actualizaciones del martes de parches de febrero de 2021.

Sin embargo, según el pronóstico de Naceri en junio de 2021, no solo se podía omitir el parche para lograr el mismo objetivo, el investigador descubrió este mes que la vulnerabilidad parcheada de forma incompleta también podría explotarse para obtener privilegios de administrador y ejecutar código malicioso en máquinas con Windows 10 que ejecutan las últimas actualizaciones de seguridad.

> *«Es decir, como nos ha enseñado HiveNightmare/SeriousSAM, una divulgación de archivo arbitraria se puede actualizar a una escalada de privilegios local si sabe qué archivos llevar y qué hacer con ellos»*, dijo el cofundador de 0patch, Mitja Kolsek.

Cabe mencionar que la vulnerabilidad se puede aprovechar para lograr la escalada de privilegios solo en circunstancias específicas, es decir, cuando la función de protección del sistema está habilitada en C:Drive, y al menos una cuenta de administrador local está configurada en la computadora.

Ni los servidores de Windows ni los sistemas que ejecutan Windows 11 se ven afectados por la vulnerabilidad, pero las siguientes versiones de Windows 10 sí se ven afectadas:

- Windows 10 v21H1 (32 y 64 bits) actualizado con actualizaciones de noviembre de 2021
- Windows 10 v20H2 (32 y 64 bits) actualizado con actualizaciones de noviembre de 2021
- Windows 10 v2004 (32 y 64 bits) actualizado con actualizaciones de noviembre de 2021
- Windows 10 v1909 (32 y 64 bits) actualizado con actualizaciones de noviembre de 2021
- Windows 10 v1903 (32 y 64 bits) actualizado con actualizaciones de noviembre de 2021
- Windows 10 v1809 (32 y 64 bits) actualizado con actualizaciones de mayo de 2021

CVE-2021-24084 es la tercera vulnerabilidad de día cero de Windows que vuelve a aparecer como consecuencia de un parche incompleto emitido por Microsoft. A inicios de este mes, 0patch envió correcciones no oficiales para una vulnerabilidad de escalamiento de privilegios local (CVE-2021-34484) en el Servicio de Perfiles de Usuario de Windows, que permite a los atacantes obtener privilegios de SISTEMA.

La semana pasada, Naceri reveló detalles de otra vulnerabilidad de día cero en el servicio Microsoft Windows Installer (CVE-2021-41379), que podría omitirse para lograr privilegios elevados en dispositivos que ejecutan las últimas versiones de Windows, incluidos Windows 10, Windows 11 y Windows Server 2022.