Microsoft ha confirmado oficialmente que se encuentra trabajando en una actualización de seguridad para corregir una vulnerabilidad de día cero en Defender, identificada bajo el nombre de *RoguePlanet*.

La falla ha recibido el identificador CVE-2026-50656 y una puntuación CVSS de 7,8. La compañía la clasifica como una vulnerabilidad de escalada de privilegios.

«Microsoft tiene conocimiento de una vulnerabilidad de elevación de privilegios en Microsoft Malware Protection Engine de Microsoft Defender, conocida públicamente como 'RoguePlanet'», indicó la empresa. *«Estamos desarrollando una actualización de seguridad de alta calidad que permita solucionar este problema.»*

La revelación se produce casi una semana después de que el investigador de seguridad Chaotic Eclipse (también conocido como Nightmare-Eclipse) publicara detalles sobre RoguePlanet, describiendo el exploit como un caso de condición de carrera (*race condition*) capaz de proporcionar a un atacante una consola con privilegios de nivel SYSTEM.

«El exploit se basa en una condición de carrera, por lo que su éxito puede variar entre intentos», explicó el investigador. *«He conseguido una tasa de éxito del 100 % en algunos equipos, mientras que en otros sistemas su funcionamiento ha resultado mucho más inconsistente.»*

En una actualización compartida el martes, el investigador añadió: *«Olvidé mencionar un detalle: sorprendentemente, la prueba de concepto (PoC) de RoguePlanet funciona independientemente de que la protección en tiempo real esté activada o desactivada, lo cual resulta bastante curioso. También sospecho que podría funcionar en modo pasivo, aunque no lo he comprobado mediante pruebas.»*

La semana pasada, Microsoft declaró que estaba al tanto de los informes relacionados con la vulnerabilidad y que se encontraba *«investigando activamente la validez y el posible alcance de estas afirmaciones.»*

RoguePlanet representa la cuarta vulnerabilidad de Microsoft Defender divulgada por Chaotic Eclipse. Anteriormente, el investigador había dado a conocer BlueHammer (CVE-2026-33825), UnDefend (CVE-2026-45498) y RedSun (CVE-2026-41091), todas ellas corregidas posteriormente por Microsoft mediante actualizaciones de seguridad.