La Agencia de Ciberseguridad e Infraestructura de los Estados Unidos (CISA) anunció el miércoles la inclusión de dos vulnerabilidades en su catálogo de Vulnerabilidades Conocidas Explotadas (KEV) debido a que están siendo activamente explotadas, al mismo tiempo que eliminó cinco errores de la lista debido a la falta de pruebas sólidas.

Las nuevas vulnerabilidades añadidas son las siguientes:

- CVE-2023-42793 (puntuación CVSS: 9.8) – Vulnerabilidad de Omisión de Autenticación en JetBrains TeamCity
- CVE-2023-28229 (puntuación CVSS: 7.0) – Vulnerabilidad de Elevación de Privilegios en el Servicio de Aislamiento de Claves CNG de Microsoft Windows

CVE-2023-42793 se refiere a una grave vulnerabilidad de omisión de autenticación que permite la ejecución remota de código en el servidor TeamCity. Datos recopilados por GreyNoise han revelado intentos de explotación de esta vulnerabilidad desde 74 direcciones IP únicas hasta la fecha.

Por otro lado, CVE-2023-28229 es una vulnerabilidad de alta gravedad en el Servicio de Aislamiento de Claves Criptográficas de Próxima Generación (CNG) de Microsoft Windows que permite a un atacante obtener privilegios SYSTEM específicos y limitados.

Hasta el momento, no existen informes públicos que documenten la explotación activa de esta vulnerabilidad en entornos en la naturaleza, y CISA no ha proporcionado más detalles sobre los ataques o los escenarios de explotación. Un «proof-of-concept» (PoC) estuvo disponible a principios del mes pasado.

Microsoft, por su parte, calificó CVE-2023-28229 como *«Menos Probable de Ser Explotada»*. Esta vulnerabilidad fue parcheada por el gigante tecnológico como parte de las actualizaciones del *«Patch Tuesday»* lanzadas en abril de 2023.

La agencia de ciberseguridad ha retirado también cinco vulnerabilidades que afectaban al dispositivo Owl Labs Meeting del catálogo KEV, alegando que no se disponía de evidencia

suficiente para mantenerlas en la lista.

Dado que se están explotando activamente dos de estas vulnerabilidades, se requiere que las agencias del Poder Ejecutivo Civil Federal (FCEB) apliquen los parches proporcionados por el proveedor antes del 25 de octubre de 2023, con el fin de asegurar sus redes contra posibles amenazas.