La Agencia de Seguridad Cibernética y de Infraestructura de EE. UU. (CISA) ha alertado sobre una vulnerabilidad de seguridad en el software de gestión de activos Trimble Cityworks, el cual está siendo explotado activamente.

El problema identificado es CVE-2025-0994 (calificación CVSS v4: 8.6), un error de deserialización de datos no confiables que podría permitir a un atacante ejecutar código de manera remota.

> *«Esto podría posibilitar que un usuario autenticado lleve a cabo un ataque de ejecución remota de código contra el servidor web Microsoft Internet Information Services (IIS) de un cliente»*, explicó CISA en un informe publicado el 6 de febrero de 2025.

Las versiones afectadas son las siguientes:

- Cityworks (Todas las ediciones anteriores a la 15.8.9)
- Cityworks con Office Companion (Todas las versiones previas a la 23.10)

A pesar de que Trimble lanzó parches de seguridad el 29 de enero de 2025 para corregir este problema, CISA ha advertido que la falla ya está siendo aprovechada en ataques reales.

La compañía con sede en Colorado también informó que ha recibido reportes sobre *«intentos no autorizados de acceso a despliegues específicos de Cityworks».*

Según los indicadores de compromiso (IoCs) publicados por Trimble, los atacantes están explotando la vulnerabilidad para instalar un cargador desarrollado en Rust, el cual ejecuta Cobalt Strike y una herramienta de acceso remoto basada en Go llamada VShell, además de otras cargas útiles no identificadas.

Por ahora, se desconoce quién está detrás de estos ataques y cuál es su propósito final. Se recomienda a los usuarios que utilicen versiones afectadas del software actualizarlo a la

última versión disponible para garantizar la máxima protección.

Actualización

En otro boletín, CISA incorporó la vulnerabilidad CVE-2025-0994 en su lista de Vulnerabilidades Explotadas Conocidas (KEV, por sus siglas en inglés), ordenando a las agencias de la Rama Ejecutiva Civil Federal (FCEB) mitigar el fallo antes del 28 de febrero de 2025.

> *«CISA urge a los administradores y usuarios a revisar los indicadores de compromiso (IoCs) y a implementar las actualizaciones y medidas de mitigación necesarias»*, señaló la agencia.