La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) añadió el lunes una vulnerabilidad de gravedad media que afecta a Wing FTP a su catálogo de Vulnerabilidades Conocidas Explotadas (KEV), tras detectar indicios de explotación activa.

La vulnerabilidad, CVE-2025-47813 (puntuación CVSS: 4.3), consiste en una falla de divulgación de información que expone la ruta de instalación de la aplicación bajo determinadas circunstancias.

Wing FTP Server presenta una vulnerabilidad en la generación de mensajes de error que contienen información sensible cuando se utiliza un valor largo en la cookie UID, señaló CISA.

El problema afecta a todas las versiones del software hasta la 7.4.3 inclusive. Fue corregido en la versión 7.4.4, publicada en mayo tras una divulgación responsable por parte del investigador Julien Ahrens de RCE Security.

Cabe mencionar que la versión 7.4.4 también soluciona CVE-2025-47812 (CVSS: 10.0), otra vulnerabilidad crítica en el mismo producto que permite la ejecución remota de código. Desde julio de 2025, esta falla ha sido explotada activamente en entornos reales.

Según información compartida en su momento por Huntress, los atacantes han aprovechado esta vulnerabilidad para descargar y ejecutar archivos Lua maliciosos, realizar tareas de reconocimiento e instalar software de monitoreo y gestión remota.

Ahrens, en una prueba de concepto (PoC) publicada en GitHub, explicó que el endpoint "/loginok.html" no valida correctamente el valor de la cookie de sesión "UID". Como consecuencia, si el valor proporcionado supera la longitud máxima permitida por el sistema operativo, se genera un mensaje de error que revela la ruta completa del servidor local.

La explotación exitosa puede permitir a un atacante autenticado obtener la ruta local del servidor de la aplicación, lo que facilita la explotación de otras vulnerabilidades como CVE-2025-47812, añadió el investigador.

Por el momento, no hay detalles claros sobre cómo se está explotando esta vulnerabilidad en ataques reales ni si se está combinando con CVE-2025-47812. Ante esta situación, se recomienda a las agencias del Federal Civilian Executive Branch (FCEB) aplicar las actualizaciones necesarias antes del 30 de marzo de 2026.