Especialistas en ciberseguridad han descubierto una nueva vulnerabilidad de seguridad de alta severidad en el software de gestión de impresión PaperCut para Windows, que podría resultar en la ejecución remota de código en circunstancias específicas.

Identificado como CVE-2023-39143 (calificación CVSS: 8.4), el defecto afecta a las versiones anteriores a 22.1.3 de PaperCut NG/MF. Se describe como una combinación de una vulnerabilidad de travesía de ruta y carga de archivos.

> *«CVE-2023-39143 permite a atacantes no autenticados potencialmente leer, eliminar y cargar archivos arbitrarios en el servidor de la aplicación PaperCut MF/NG, lo que resulta en la ejecución remota de código en ciertas configuraciones»,* dijo Naveen Sunkavally de Horizon3.ai

La empresa de ciberseguridad explicó que la carga de archivos que conduce a la ejecución remota de código es posible cuando está habilitada la configuración de integración con dispositivos externos, que viene activada por defecto en algunas instalaciones de PaperCut.

A principios de abril, otra vulnerabilidad de ejecución remota de código en el mismo producto (CVE-2023-27350, calificación CVSS: 9.8) y una falla de divulgación de información (CVE-2023-27351) fueron ampliamente explotadas en la naturaleza para distribuir Cobalt Strike y ransomware. También se detectó que actores estatales de Irán abusaron de estas vulnerabilidades para obtener acceso inicial a redes objetivo.

En comparación con CVE-2023-27350, CVE-2023-39143 tampoco exige que los atacantes posean privilegios previos para explotarlo, y no se necesita ninguna interacción por parte del usuario, observó Sunkavally. *«CVE-2023-39143 es más complejo de aprovechar, ya que implica múltiples problemas que deben combinarse para comprometer un servidor. No se trata de una vulnerabilidad de ejecución remota de código (RCE) de un solo paso».*

Además, corregido por PaperCut en la versión 22.1.3, existe un fallo de seguridad que podría permitir a un atacante no autenticado con acceso directo a la IP del servidor cargar archivos

arbitrarios en un directorio objetivo, lo que podría resultar en un potencial ataque de denegación de servicio (CVE-2023-3486, calificación CVSS: 7.4). Tenable ha sido reconocido por descubrir y reportar este problema.