Investigadores de seguridad cibernética revelaron el martes fallas de seguridad de ocho años que afectan a 150 impresoras multifuncionales (MFP) diferente de HP Inc. y que podrían ser abusadas por un adversario para tomar el control de dispositivos vulnerables, robar información confidencial e infiltrarse en redes empresariales para montar otros ataques.

Los investigadores de F-Secure Labs, Timo Hirvonen y Alexander Bolshev, descubrieron y notificaron a HP las dos vulnerabilidades, denominadas colectivamente como Printing Shellz, el 29 de abril de 2021, lo que llevó a la compañía a publicar parches a inicios de noviembre.

- CVE-2021-39237 (puntuación CVSS de 7.1): Una vulnerabilidad de divulgación de información que afecta a determinadas impresoras HP LaserJet, HP LaserJet Managed, HP PageWide y HP PageWide Managed.
- CVE-2021-39238 (puntuación CVSS de 9.3): Una vulnerabilidad de desbordamiento de búfer que afecta a determinados productos HP Enterprise LaserJet, HP LaserJet Managed, HP Enterprise PageWide y HP PageWide Managed.

> *«Las fallas están en el panel de comunicaciones de la unidad y en el analizador de fuentes. Un atacante puede explotarlos para obtener derechos de ejecución de código; el primero requiere acceso físico, mientras que el segundo se puede lograr remotamente. un ataque exitoso permitirá que un atacante logre varios objetivos, incluido el robo de información o el uso de la máquina comprometida como cabeza de playa para futuros ataques contra una organización»,* dijeron Hirvonen y Bolshev.

La clasificación de gravedad crítica de CVE-2021-39238 también se debe a que la vulnerabilidad se puede eliminar con gusanos, lo que significa que podría explotarse para autopropagarse a otras MPF en la red comprometida.

Un escenario de ataque hipotético podría implicar la incorporación de un exploit para los defectos de análisis de fuentes en un documento PDF malicioso y luego la ingeniería social del objetivo para que imprima el archivo.

De forma alternativa, un empleado de la organización víctima podría ser atraído para que visite un sitio web fraudulento en el proceso, enviando el exploit al MPF vulnerable directamente desde el navegador web en lo que se conoce como un ataque de impresión entre sitios.

> *«El sitio web imprimiría, automáticamente, de forma remota un documento que contenga una fuente creada con fines malintencionados en el MPF vulnerable, dando al atacante los derechos de ejecución del código en el dispositivo»,* dijeron los investigadores.

Además de imponer la segmentación de la red y deshabilitar la impresión desde unidades USB de forma predeterminada, se recomienda a las organizaciones que utilizan los dispositivos afectados que instalen los parches lo más pronto posible.

> *«Si bien explotar estos problemas es algo difícil, la divulgación pública de estas vulnerabilidades ayudará a los actores de amenazas a saber qué buscar para atacar a las organizaciones vulnerables»,* dijeron los investigadores.