BOLETÍN DE ALERTA

Boletín Nro.: 2021-33

Fecha de publicación: 01/12/2021

Tema: Vulnerabilidad de desbordamiento de búfer en varios productos de impresoras HP

Productos Afectados:

- HP Color LaserJet Enterprise
- HP Color LaserJet Enterprise Flow
- HP Color LaserJet Managed Flow
- HP Color LaserJet Managed
- HP Color LaserJet Managed MFP
- HP Color LaserJet Pro
- HP Digital Sender Flow
- HP PageWide
- HP PageWide Enterprise
- HP PageWide Managed
- HP PageWide Pro
- HP Scanjet Enterprise
- El listado completo de los 174 dispositivos afectados se encuentra aquí.

Descripción:

La vulnerabilidad CVE-2021-39238 de desbordamiento de búfer clasificada como crítica, con una puntuación de 9.8, fue encontrada en las líneas de HP Enterprise LaserJet, LaserJet Managed, Enterprise PageWide y Enterprise PageWide Managed.

Esta vulnerabilidad se encuentra relacionada a una función de lectura del tipo de fuente de letra dentro del código del firmware de las impresoras afectadas. Esto repercutiría sobre la confidencialidad, integridad y disponibilidad del dispositivo.

El método de ataque consiste en engañar a un usuario de una organización para que visite un sitio web malicioso que manipulará la impresora multifunción vulnerable configurada en el equipo de la víctima a través de un ataque *Cross Site Printing*. El sitio web enviaría la orden

de impresión remota de un documento que contenga una fuente de letra maliciosa (con código malicioso)

Impacto:

La explotación exitosa de esta vulnerabilidad otorgaría al atacante los permisos de ejecución de código en el dispositivo incluyendo no solo acceso a los documentos impresos, escaneados o enviados por fax, sino también a información como credenciales de acceso a la impresora; adicionalmente podría ser utilizada como *pivot* dentro de la red de la víctima.

Detección:

- De acuerdo con los investigadores la detección puede realizarse a través de monitoreo de tráfico y análisis de *logs*.

Solución:

Verificar que el firmware de su dispositivo HP se encuentre actualizado; pudiendo descargar el firmware actualizado del sitio oficial de HP:

- https://support.hp.com/us-en/drivers

Información adicional:

- https://vuldb.com/es/?id.185937
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39238
- https://nvd.nist.gov/vuln/detail/CVE-2021-39238
- https://support.hp.com/us-en/document/ish_5000383-5000409-16