BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-42
Fecha de publicación: 26/09/2024
Tema: Multiples Vulnerabilidades en CUPS Linux
Traffic Light Protocol (TLP): White

Producto(s) afectado:

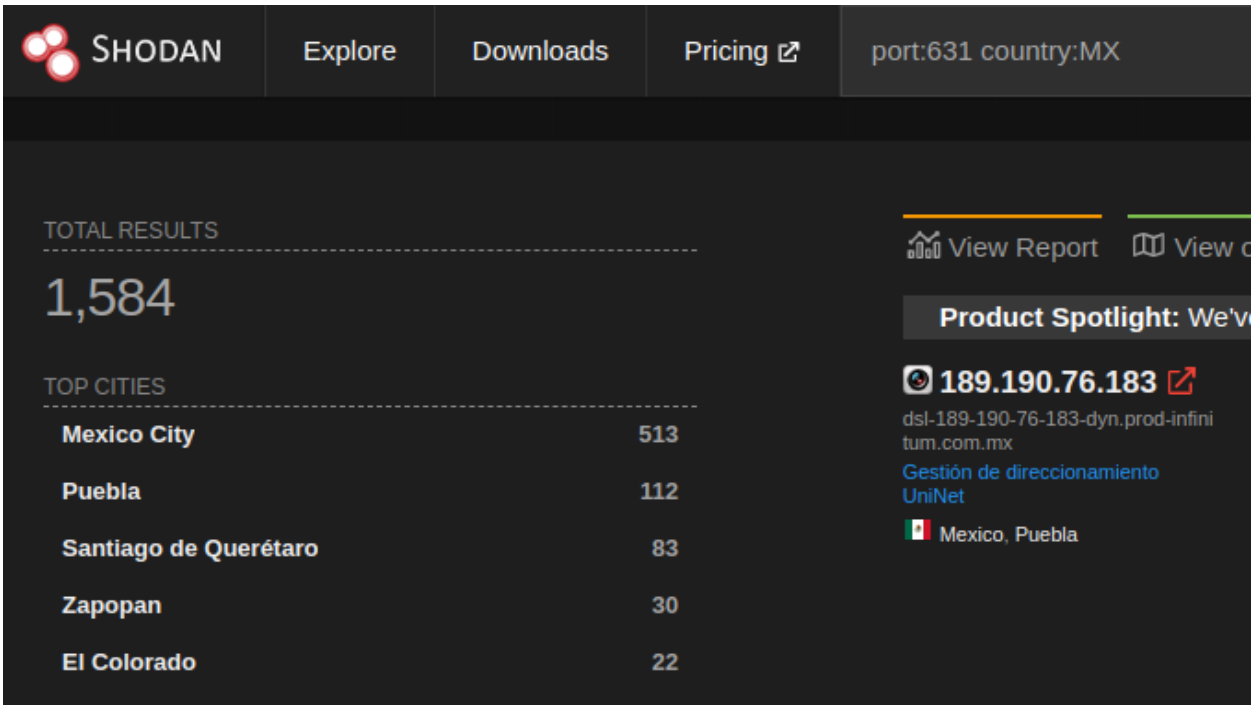
- cups-browsed <= 2.0.1, libcupsfilters <= 2.1b1, libppd <= 2.1b1 y cups-filters <= 2.0.1

Descripción

Se han identificado varias vulnerabilidades críticas en CUPS (Common UNIX Printing System), afectando a varias versiones de Linux, incluidas todas las versiones de Red Hat Enterprise Linux (RHEL), aunque no en su configuración predeterminada. Las vulnerabilidades permiten la ejecución remota de código (RCE) en sistemas vulnerables.

Las vulnerabilidades afectan a la funcionalidad de impresión en sistemas Linux, permitiendo que un atacante remoto no autenticado ejecute comandos arbitrarios en el sistema. Entre las vulnerabilidades, destaca que el servicio cups-browsed permite la creación de impresoras maliciosas a través de la red cuando está habilitado, lo cual no es la configuración predeterminada.

Se detecto que en México casi 1.600 equipos pueden estar expuestos a la explotación de estas vulnerabilidades. Es posible que varios de dichos dispositivos sean router o dispositivos de red, además de servidores.



Las vulnerabilidades críticas identificadas son:

- CVE-2024-47176: cups-browsed ≤ 2.0.1 escucha en el puerto UDP 631 y permite a un atacante controlar peticiones IPP.
- CVE-2024-47076: libcupsfilters ≤ 2.1b1 no valida correctamente los atributos IPP, permitiendo la inyección de datos maliciosos.
- CVE-2024-47175: libppd ≤ 2.1b1 no valida los atributos IPP cuando los escribe en archivos PPD, permitiendo la inyección de datos maliciosos.
- CVE-2024-47177: cups-filters ≤ 2.0.1 permite la ejecución de comandos arbitrarios a través del parámetro FoomaticRIPCommandLine.

Solución

Red Hat y otros distribuidores de Linux han proporcionado instrucciones para mitigar estas vulnerabilidades. Se recomienda lo siguiente:

- Deshabilitar y eliminar el servicio cups-browsed si no se utiliza.
- Actualizar el paquete CUPS a la última versión disponible en el sistema.
- Si no es posible actualizar el sistema y se depende del servicio, bloquear el tráfico UDP hacia el puerto 631 y, de ser necesario, todo el tráfico DNS-SD.

Estas acciones evitarán que los atacantes exploten remotamente las vulnerabilidades y protegerán los sistemas de posibles ataques de ejecución remota de código.

Información adicional:

- https://github.com/OpenPrinting/cups-browsed/issues/36?ref=thestack.technology
- https://www.evilsocket.net/2024/09/26/Attacking-UNIX-systems-via-CUPS-Part-I/?ref=thestack.technology
- https://www.redhat.com/en/blog/red-hat-response-openprinting-cups-vulnerabilities
- https://www.cve.org/CVERecord?id=CVE-2024-47176

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com