## I. DATOS GENERALES:

**Clase de alerta:** Vulnerabilidad

**Tipo de incidente:** Ataques remotos sin autenticación

**Nivel de riesgo:** Alto

## II. ALERTA

El investigador de seguridad Simone Margaritelli ha identificado una vulnerabilidad de seguridad crítica que afecta a todos los sistemas GNU/Linux (y potencialmente a otros). La vulnerabilidad tiene una puntuación de 9,9/10 en la escala de gravedad CVSS y permite la ejecución remota de código RCE sin autenticación.

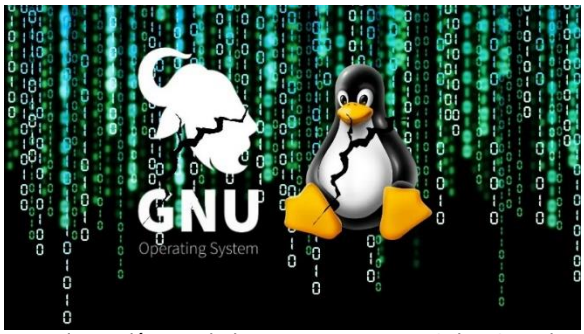


**Figura 1.-** *Ilustración asociada a LINUX.* ***Fuente:*** *Cyber Security News*

## III. INTRODUCCIÓN

CUPS (abreviatura de Common UNIX Printing System) es el sistema de impresión de código abierto más utilizado en sistemas Linux que se basa en el Protocolo de impresión de Internet (IPP), compatible con dispositivos que ejecutan sistemas operativos tipo Unix, como FreeBSD, NetBSD y OpenBSD y sus derivados.

Varias vulnerabilidades de CUPS sin parchear que pueden encadenarse para lograr la ejecución remota de código abierto fueron encontradas y reportadas por el desarrollador de software Simone Margaritelli, quien ahora ha revelado abiertamente las debilidades de seguridad.

Si se utiliza el sistema de impresión Unix CUPS con cups-browsed habilitado una computadora puede ser vulnerable. Los ataques requieren que la víctima inicie un trabajo de impresión. Cabe mencionar que estas fallas de seguridad no afectan a los sistemas en su configuración predeterminada.

Shadowserver ha reportado que en el Ecuador se ha identificado siete (7) casos relacionados de la vulnerabilidad IPP.

**Figura 2.** Reporte de detecciones.
**Fuente: https**: https://dashboard.shadowserver.org/statistics/combined/tree/?day=2024-09-26&source=scan&source=scan6&tag=ipp&geo=AG%2CAR%2CAW%2CBZ%2CBO%2CBQ%2CBR%2CCL%2CCO%2CCR%2CCU%2CCW%2CDO%2CEC%2CSV%2CFK%2CGF%2CGT%2CGY%2CHT%2CHN%2CMX%2CNI%2CPA%2CPY%2CPE%2CMF%2CSX%2CGS%2CSR%2CTT%2CUY%2CVE&data_set=count&scale=log

## IV. VECTOR DE ATAQUE:

El investigador Margaritelli descubrió que si el demonio cups-browsed está habilitado, escuchará en el puerto UDP 631 y permitirá de manera predeterminada, conexiones remotas desde cualquier dispositivo de la red para crear una nueva impresora enviando un paquete UDP especialmente diseñado a una instancia vulnerable de CUPS con conectividad a Internet solicitando que se agregue una impresora. La "impresora" especificada por el atacante es en realidad la dirección del objetivo y CUPS le enviará una solicitud IPP/HTTP.

Además, se descubrió que se podía crear una impresora PostScript Printer Description (PPD) maliciosa que podía anunciarse manualmente a un servicio cups-browsed expuesto en el puerto UDP 631. Esto hace que la máquina remota instale automáticamente la impresora maliciosa y la ponga a disposición para imprimir. Si el usuario de ese servidor expuesto imprime en la nueva impresora, el comando malicioso del PPD se ejecutará localmente en la computadora.

Este comando malicioso del PPD, se agrega a través de un filtro foomatic-rip , que ejecuta comandos en un dispositivo para que un trabajo de impresión se represente correctamente.

```
1  # ... other configuration removed for brevity ...
2
3  # enables the IPP server
4  ipp:
5      # this can be the name of an existing device
6      # in which case its original IPP record will be transparently hijacked
7      printer-name: EVIL_PRINTER
8
9      # where the magic happens, it's important to preserve the new lines
10     printer-privacy-policy-uri: |
11         https://www.google.com/"
12         *FoomaticRIPCommandLine: "echo 1 > /tmp/PWNED"
13         *cupsFilter2 : "application/pdf application/vnd.cups-postscript 0 foomatic-rip
```

**Figura 3:** Comandos añadidos mediante el filtro foomatic-rip (Simone Margaritelli)

Por otro lado, a empresa Akamai descubrió que por cada paquete enviado, el servidor CUPS vulnerable generará una solicitud IPP/HTTP más grande y

parcialmente controlada por el atacante dirigida al objetivo especificado. Como resultado, no solo se ve afectado el objetivo, sino que el host del servidor CUPS también se convierte en víctima, ya que el ataque consume su ancho de banda de red y recursos de CPU.

En determinadas condiciones, los atacantes pueden encadenar un conjunto de vulnerabilidades en múltiples componentes del sistema de impresión de código abierto CUPS para ejecutar código arbitrario de forma remota en máquinas vulnerables rastreadas como:

- **CVE-2024-47076 (libcupsfilters),** *hasta la versión 2.1b1 cfGetPrinterAttributes*. No valida ni desinfecta los atributos IPP devueltos desde un servidor IPP, proporcionando datos controlados por el atacante al resto del sistema CUPS.

- **CVE-2024-47175 (libppd)**, hasta la versión 2*.1b1 ppdCreatePPDFromIPP2*. No valida ni desinfecta los atributos IPP al escribirlos en un archivo PPD temporal, lo que permite la inyección de datos controlados por el atacante en el PPD resultante.

- **CVE-2024-47176 (cups-browsed)**, hasta la versión 2.0.1 se vincula a UDP INADDR_ANY:631 y confía en cualquier paquete de cualquier origen para activar una *Get-Printer-Attributes* solicitud IPP a una URL controlada por el atacante; y

- **CVE-2024-47177 (cups-filters),** hasta la versión 2.0.1 *foomatic-rippermite* la ejecución de comandos arbitrarios a través del *FoomaticRIPCommandLine* parámetro PPD.

## V. IMPACTO:

Si bien se trata de una cadena de ejecución remota de código, se debe considerar que los atacantes deben superar algunos obstáculos para explotar las vulnerabilidades y lograr la ejecución remota de código.

El primero es que los sistemas atacados deben tener expuesto el protocolo IPP (Internet Printing Protocol) y habilitado el demonio cups-browsed que normalmente no está habilitado de forma predeterminada.

Luego, el atacante debe engañar a un usuario para que imprima desde un servidor de impresora malicioso en su red local que aparece de repente en su máquina. Un atacante remoto no autenticado puede reemplazar silenciosamente las URL IPP de impresoras existentes (o instalar nuevas) con una maliciosa, lo que resulta en la ejecución de comandos arbitrarios cuando se inicia un trabajo de impresión desde la computadora víctima.

Además, el atacante puede usar relleno para hacer estas solicitudes aún más grandes y amplificar aún más el ataque.

## VI. RECOMENDACIONES:

- Identificar si el servicio cups-browsed está activo aplicando el comando: "***systemctl status cups";*** Si el resultado muestra "Activo: inactivo (muerto)", entonces la cadena de explotación se detiene y el sistema no es vulnerable. Si el resultado muestra "en ejecución" o "habilitado" y la directiva "BrowseRemoteProtocols" contiene el valor "cups" en el archivo de configuración /etc/cups/cups-browsed.conf, entonces el sistema es vulnerable.

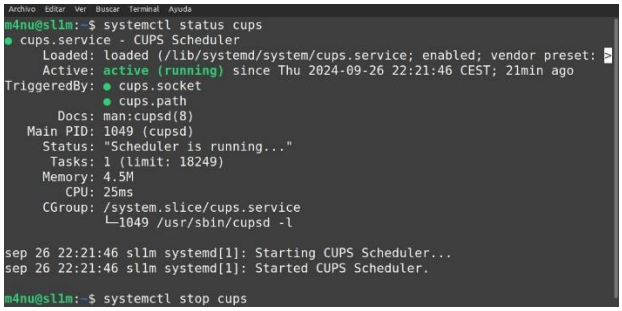


**Figura 4.** Comando: "systemctl status cups". **Fuente:** Cuenta X - @CiberPoliES

- Ejecute el comando " **systemctl stop cups-browsed**" para pararlo; "**systemctl disable cups-browsed**" para deshabilitarlo si el servicio no es necesario.

- En caso de que su red requiera de este servicio habilitado, bloquee todo el tráfico al puerto TCP/UDP 631 y tráfico DNS-SD al internet.
- Mantenerse informado sobre nuevas vulnerabilidades asociadas de fuentes confiables.
- Revisar y mejorar las medidas de seguridad existentes en firewalls, sistemas de detección de intrusos.

## VII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

## VIII. REFERENCIAS:


- https://www.managedserver.eu/very-serious-vulnerability-on-linux-unknown-for-now-discovered-by-evilsocket/
- https://cybersecuritynews.com/critical-unauthenticated-rce-flaw/
- https://x.com/CiberPoliES/status/1839409210909749383?t=ZbtdU7qbMrVwoIsu--A_IA&s=08
- https://www.bleepingcomputer.com/news/security/cups-flaws-enable-linux-remote-code-execution-but-theres-a-catch/
- https://www.securityweek.com/after-code-execution-researchers-show-how-cups-can-be-abused-for-ddos-attacks/
- https://www.bleepingcomputer.com/news/security/cups-flaws-enable-linux-remote-code-execution-but-theres-a-catch/