Se ha informado sobre un nuevo conjunto de vulnerabilidades de seguridad en el sistema de impresión OpenPrinting Common Unix Printing System (CUPS) para sistemas Linux, las cuales podrían permitir la ejecución remota de comandos bajo ciertas circunstancias.

> *«Un atacante remoto no autenticado puede cambiar silenciosamente las URLs IPP de impresoras existentes (o instalar nuevas) por una maliciosa, lo que provoca la ejecución arbitraria de comandos (en el equipo) cuando se inicia una tarea de impresión desde ese equipo»,* explicó el investigador de seguridad Simone Margaritelli.

CUPS es un sistema de impresión de código abierto y basado en estándares, utilizado en Linux y otros sistemas operativos similares a Unix, como ArchLinux, Debian, Fedora, Red Hat Enterprise Linux (RHEL), ChromeOS, FreeBSD, NetBSD, OpenBSD, openSUSE y SUSE Linux.

El listado de vulnerabilidades es el siguiente:

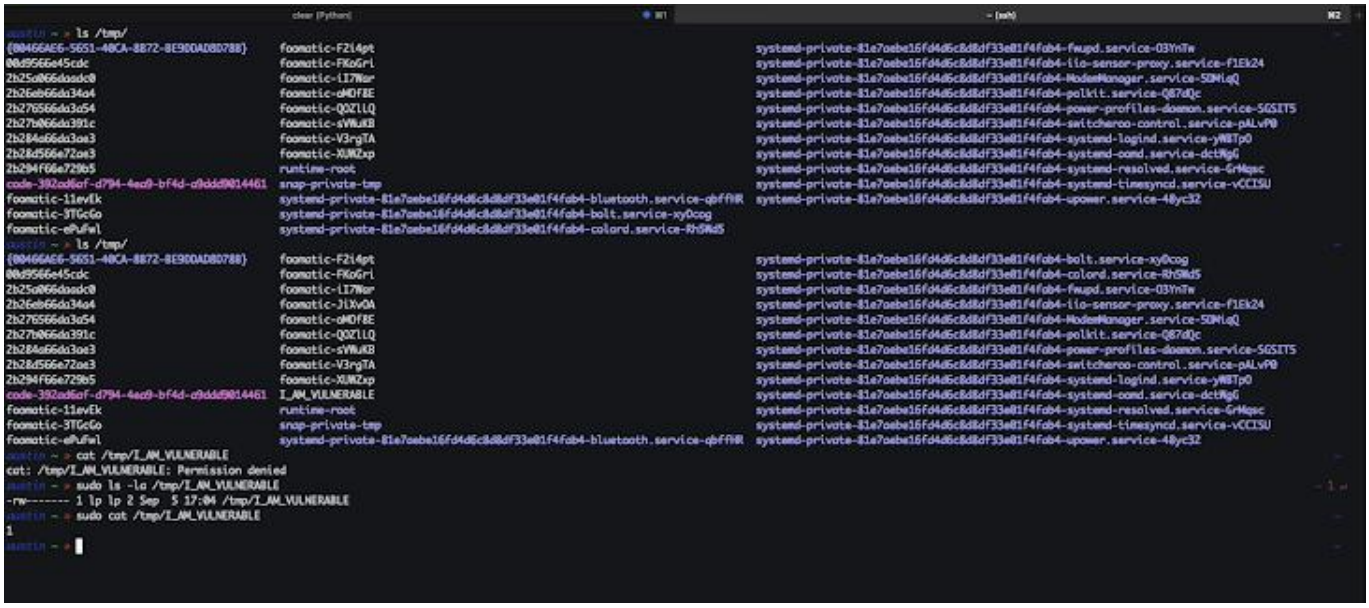
- CVE-2024-47176: cups-browsed <= 2.0.1 se conecta a UDP INADDR_ANY:631, confiando en cualquier paquete de cualquier origen para ejecutar una solicitud Get-Printer-Attributes IPP a una URL bajo el control del atacante.
- CVE-2024-47076: libcupsfilters <= 2.1b1 cfGetPrinterAttributes5 no valida ni limpia los atributos IPP que recibe de un servidor IPP, lo que permite que el sistema CUPS procese datos manipulados por el atacante.
- CVE-2024-47175: libppd <= 2.1b1 ppdCreatePPDFromIPP2 no realiza una verificación adecuada de los atributos IPP al escribirlos en un archivo PPD temporal, lo que facilita la inyección de datos controlados por el atacante en el archivo resultante.
- CVE-2024-47177: cups-filters <= 2.0.1 foomatic-rip permite la ejecución de comandos arbitrarios a través del parámetro FoomaticRIPCommandLine en los archivos PPD.

Como resultado de estas vulnerabilidades, es posible construir una cadena de exploits que permita a un atacante crear un dispositivo de impresión falso en un sistema Linux expuesto a la red que ejecute CUPS, y ejecutar código malicioso de forma remota al enviar un trabajo de

impresión.

> *«El problema surge debido al manejo incorrecto de los anuncios de 'Nueva Impresora Disponible' en el componente 'cups-browsed', sumado a la validación deficiente de 'cups' sobre la información proporcionada por un recurso de impresión malicioso»*, mencionó la empresa de seguridad Ontinue.
>
> *«La falla radica en la validación insuficiente de los datos de la red, lo que posibilita que un atacante instale un controlador de impresora malicioso en el sistema vulnerable y luego envíe un trabajo de impresión que desencadene la ejecución de código malicioso. Este código se ejecuta con los permisos del usuario 'lp', y no del superusuario 'root'.»*

Red Hat Enterprise Linux (RHEL), en un aviso, señaló que todas las versiones de su sistema operativo se ven afectadas por estos fallos, pero aclaró que no son vulnerables en su configuración por defecto. Clasificó las vulnerabilidades como de importancia alta, aunque el impacto en escenarios reales probablemente sea limitado.



> *«Al combinar este grupo de vulnerabilidades, un atacante podría lograr la ejecución remota de código, lo que podría derivar en el robo de información sensible o daños en sistemas críticos de producción»*, indicó RHEL.

La firma de ciberseguridad Rapid7 subrayó que los sistemas vulnerables solo son explotables si el puerto UDP 631 está abierto y el servicio vulnerable está en escucha, ya sea desde la internet pública o a través de segmentos de red.

Palo Alto Networks informó que ninguno de sus productos ni servicios en la nube incluye los paquetes de software relacionados con CUPS, por lo que no se ven afectados por estos fallos.

Actualmente se están desarrollando parches para corregir las vulnerabilidades, y se espera que estén disponibles en los próximos días. Mientras tanto, se recomienda deshabilitar y eliminar el servicio cups-browsed si no es necesario, además de bloquear o restringir el tráfico hacia el puerto UDP 631.

> *«Todo parece indicar que las vulnerabilidades no autenticadas en Linux, que han sido descritas como catastróficas para los sistemas Linux, probablemente solo afecten a una fracción de los sistemas»,* declaró Benjamin Harris, CEO de WatchTowr.
>
> *«Dado esto, aunque las vulnerabilidades son graves en términos técnicos, es menos probable que las máquinas de escritorio o estaciones de trabajo que ejecutan CUPS estén expuestas a internet de la misma manera o en los mismos volúmenes que las ediciones de servidores Linux.»*

Satnam Narang, ingeniero investigador senior en Tenable, comentó que estas vulnerabilidades no alcanzan el nivel de gravedad de Log4Shell o Heartbleed.

> *«La realidad es que en el mundo del software, ya sea de código abierto o cerrado, hay una cantidad incontable de vulnerabilidades que aún no han sido descubiertas ni reveladas. La investigación en seguridad es esencial en este proceso, y debemos exigir más a los proveedores de software»*, comentó Narang.
>
> *«Para las organizaciones que están abordando estas vulnerabilidades recientes, es crucial destacar que las fallas más preocupantes son las vulnerabilidades conocidas que siguen siendo explotadas por grupos avanzados de amenazas persistentes con vínculos a estados nacionales, así como por afiliados de ransomware que extorsionan millones de dólares a las corporaciones cada año.»*