Sociedad Andaluza para el Desarrollo de las Telecomunicaciones
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

seguridad+ Y CONFIANZA DIGITAL | AndalucíaCERT CENTRO DE SEGURIDAD TIC

Informe de divulgación
Seguridad en impresoras multifunción

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-10131-170515*
Edición:	*0*
Categoría	*Público*
Fecha de elaboración:	*12/04/2017*
N° de Páginas	*1 de 13*

1 TABLA DE CONTENIDOS

2 OBJETIVO

Este documento tiene como objeto el concienciar sobre la seguridad en las impresoras, poniendo de manifiesto los vectores de ataque más comunes, así como ofrecer un conjunto de consejos para el uso y la configuración de las mismas.

3 ALCANCE

Este documento va dirigido tanto al personal de la Junta de Andalucía, como al público en general. Es de carácter divulgativo e informativo, en el cual se pretende dar a conocer los vectores de ataque existentes contra las impresoras, pero sobre todo, que el usuario sea consciente de una nociones básicas de un uso más seguro.

4 INTRODUCCIÓN

La impresora es una herramienta indispensable para la mayoría de empresas en el mundo. La evolución de la impresora ha llevado a que sean herramientas cada vez más completas y complejas, con mayores y mejores funcionalidades, como son la capacidad de escanear, fotocopiar, mandar faxes, conectarse por Wi-Fi o Bluetooth a otros dispositivos, etc.

En la mayoría de entornos, una impresora recibe, imprime, almacena o envía información sensible y confidencial. Sin embargo, en la mayoría de casos los controles implementados en el uso de las impresoras no son los apropiados para garantizar la seguridad, en ocasiones por la falta de conciencia de los peligros que una mala securización conlleva.

Para concienciar al usuario de cuáles son los peligros en las impresoras, este documento hace un estudio de los diferentes vectores de ataque contra estos dispositivos. Además, se darán una serie de recomendaciones para su correcta configuración y uso.

4.1 Evolución y tecnología en las impresoras

Desde la creación de la impresora en los años 40, estas máquinas, al principio muy básicas, han ido evolucionando conforme a las necesidades de los usuarios y a la tecnología disponible.

Las tecnologías de impresión han ido evolucionando y mejorando, ofreciendo actualmente diferentes tipos de impresoras: de inyección de tinta, láser, matricial, térmica, plotter, de rueda de margarita, etc. No sólo la tecnología de impresión ha evolucionado en las impresoras, sino también las funcionalidades que ofrecen así como su conectividad.

La primera impresora de red fue lanzada en 1991 (HP LaserJet IIIsi). Los clientes se podían conectar a ella a través de Ethernet o Token Ring a través del servidor de impresión HP JetDirect.

Años después, en 1998, encontramos el lanzamiento de la primera impresora multifuncional para el gran público (HP LaserJet 3100). Desde entonces el concepto de impresora evolucionó, ofreciendo un nuevo tipo de impresora más equipada y completa: la impresora multifunción.

Posteriormente, se han añadido otras funcionalidades y tecnologías a las impresoras: servidor web (para la administración de la impresora), servidor SMB, servidor FTP, escáner, FAX, Wi-Fi, Bluetooth, conexión con la nube, capacidad de enviar y recibir emails, etc. Cada una de estas funcionalidades es un posible vector de ataque, siendo la seguridad un factor importante y necesariamente inherente a ellas.

5 SEGURIDAD EN LAS IMPRESORAS

Hoy en día es habitual que una impresora de oficina estándar disponga de otras funciones como la de escanear, mandar faxes, conectarse a la red local y a Internet. Las impresoras son dispositivos que normalmente funcionan con sistemas Linux sobre procesadores ARM. Las impresoras son tan susceptibles al malware y a los ataques de los ciberdelincuentes como los PC. Por tanto, las impresoras deben de ser consideradas como un sistema más de nuestra red, teniendo las consideraciones necesarias en materia de seguridad.

Además, nos encontramos con el problema de la falta de concienciación de la necesidad de implantar la seguridad en las impresoras. Un estudio realizado por McAfee y Xerox[6] reveló que más de la mitad (54%) de los trabajadores admiten no seguir siempre las políticas de seguridad de su empresa. Además, la mitad (51%) reconocen haber copiado, escaneado o impreso información confidencial en el trabajo. Dicho estudio también demuestra que sólo el 6% de los empleados piensan que las impresoras multifunción representan una amenaza de seguridad, mientras que el 54% piensa que dicha amenaza reside únicamente en los PC.

Para ello, es importante conocer los vectores de ataque y conocer, en caso de materializarse la amenaza, su impacto en los activos de nuestra empresa.

5.1 Vectores de ataque

Los vectores de ataque en las impresoras son variados. Cada una de las funcionalidades y servicios que ofrece una impresora puede suponer un riesgo si no está bien securizado. Además, suelen estar accesibles físicamente para mucha gente dentro de una misma oficina, permitiendo acceder a personas que en un principio no deberían tener acceso a ellas.

Confidencialidad del documento impreso:

Cuando un usuario envía algo a imprimir desde su PC a la impresora, suele haber un lapso de tiempo entre que el documento es impreso y el usuario lo recoge. Esto deja una ventana de tiempo en la que cualquier persona del entorno puede acceder al documento impreso, el cual en muchas ocasiones contiene información confidencial y datos personales. Para solventar este problema es recomendable autenticar al usuario antes de que el documento se imprima, así se asegura la presencia del usuario en el momento de la impresión. Dicha autenticación se puede realizar mediante PIN, tarjeta RFID, etc.

Mala configuración de los servicios:

Las impresoras multifunción actuales incluyen una amplia variedad de servicios para el usuario, como el de servidor FTP, Samba, Web... Una mala configuración de estos servicios puede dar lugar a que se produzca un ataque.

Por ejemplo, si configuramos el servidor FTP para que permita iniciar sesión con el usuario "anonymous" podremos acceder al FTP de la impresora sin necesidad de contraseña.

Vulnerabilidades en los servicios:

Al igual que en los ordenadores y servidores, los servicios de las impresoras son implementaciones para el sistema operativo concreto que tenga la impresora, el cual puede contener vulnerabilidades, ya sea por el propio protocolo o por una mala implementación del mismo. Puesto que cada día se encuentran nuevas vulnerabilidades en multitud de sistemas y servicios, la probabilidad de que se encuentre una vulnerabilidad en un servicio de una impresora anticuada y desactualizada es bastante alta.

Protocolos inseguros:

Algunos protocolos se consideran inseguros al no cifrar las comunicaciones. Ejemplos de estos protocolos inseguros son HTTP (utilizado para el acceso al panel de control web de la impresora), FTP (utilizado para la impresión y transmisión de ficheros), SNMPv1 y SNMPv2.

La utilización de protocolos inseguros en las impresoras permite a un posible atacante que está capturando el tráfico de red de la impresora acceder y leer la información transmitida.

En cambio, la utilización de protocolos seguros como HTTPS y SNMPv3 (que sí cifran la comunicación), garantizan que un atacante no pueda acceder a la información capturada, al estar cifrada toda la información transmitida.

Modificación de firmware:

Al igual que en cualquier dispositivo cuyo firmware se pueda actualizar, siempre cabe la posibilidad de analizar y modificar el firmware de la impresora. Buscando en el fichero del firmware se pueden encontrar contraseñas en claro para accesos privilegiados, o encontrar un modo de saltarse el control de acceso a la impresora. Si el firmware contiene el servidor web para su administración, sería muy fácil modificar los archivos para incluir una puerta trasera, e incluso incrustar una webshell. Dichas ROMs (ficheros de firmware) se publican en sitios web maliciosos con la intención de que alguna víctima lo descargue (en vez de hacerlo desde la página oficial de su impresora, que es como se debería de hacer). Algunos fabricantes de impresoras utilizan firmas electrónicas sobre los ficheros de actualización de firmware, para validar su autenticidad y evitar este tipo de modificaciones, además de validar la integridad del firmware descargado.

Robo de información (robo de la memoria de almacenamiento):

Muchas impresoras utilizan dispositivos de almacenamiento masivo (discos duros o HDDs) para guardar los documentos en la cola de trabajo, o incluso para guardar documentos en red, los cuales contienen en muchas ocasiones información confidencial o datos personales. El acceso físico a la impresora permite la obtención del disco duro, el cual podría ser clonado y analizado a posteriori para robar la información contenida en el, o incluso ser modificado para incluir algún tipo de malware.

Además, hay que considerar que aunque la impresora borre el archivo tras ser impreso, los ficheros pueden ser recuperados con herramientas forense.

Las impresoras multifunción capaces de escanear documentos también suelen guardar los documentos escaneados en el disco duro interno, a veces como ficheros temporales, pero que pueden ser igualmente recuperados una vez borrados mediante el uso de herramientas forense.

Publicación de servicios en Internet:

Muchas impresoras, al igual que otros dispositivos que se conectan en red (como las cámaras IP), proporcionan la posibilidad de ser accedidas desde Internet, para darle la posibilidad al usuario de imprimir documentos o administrar la impresora aún cuando se encuentre fuera de su red local o corporativa. De esta forma, se publican algunos de los servicios de la impresora a Internet. Dichos servicios deben de disponer de un control de acceso, como un login en su página web de acceso, para evitar que cualquier persona acceda a la impresora y la desconfigure o acceda a información privada.

Instalación de aplicaciones maliciosas:

Algunas impresoras permiten la instalación de aplicaciones extra las cuales son descargadas de los repositorios oficiales del fabricante. Esta capacidad de modificar el sistema permite que, hackeando la impresora, se puedan instalar aplicaciones maliciosas e incluso juegos[1]. Aunque la instalación de un juego no sea algo preocupante, nos da una idea de hasta qué punto se pueden modificar estos sistemas, los cuales podrían permitir la instalación de malware como algún troyano que intercepte el tráfico, robe documentos y credenciales de acceso, o incluso que utilice la impresora como parte de una Botnet.

Contraseñas inseguras:

Como en cualquier sistema, la utilización de contraseñas seguras y únicas debe de ser obligatorio. El utilizar contraseñas poco robustas facilita los ataques de fuerza bruta. Si se utiliza la misma contraseña en todos los servicios y credenciales de la impresora, facilitamos el acceso a todos ellos en caso de producirse un robo de contraseña. Además, es recomendable no utilizar ninguna de las contraseñas de la impresora para acceder a otros sistemas. En caso de producirse un robo de credenciales de la impresora, el atacante probará dichas credenciales en otros servicios de la red, para loguearse en el equipo del usuario de forma remota o loguearse en la página web corporativa, por ejemplo.

Podemos encontrar en muchas impresoras que la mayoría de los servicios vienen activados y con las contraseñas por defecto. Conociendo el modelo de la impresora es fácil para un atacante conocer las contraseñas por defecto de los distintos servicios. Por ello es recomendable cambiar las contraseñas por defecto por contraseñas robustas.

Accesos remotos:

Algunos fabricantes reconocen poder acceder a sus dispositivos de forma remota para realizar tareas de soporte cuando son necesarias. Esto, aunque supone una facilidad para el fabricante a la hora de dar soporte a sus clientes, supone un riesgo al disponer de una puerta trasera para acceder a la impresora. Aunque dicha puerta implemente varias medidas de seguridad, podría ser utilizada con fines maliciosos.

Forzado de la mecánica y electrónica:

Las impresoras láser, en caso de verse comprometidas, tienen el riesgo añadido de ser utilizadas para incendiar el papel que utiliza para imprimir mediante el forzado del sistema mecánico y electrónico [2].
Esto se puede lograr accediendo a la impresora a bajo nivel (utilizando los drivers de la electrónica de la impresora), haciendo uso de los rodillos fusores, que son los encargados de secar la tinta una vez es aplicada al papel, para calentarlos en exceso y provocar así que se queme el papel.

Este tipo de ataques puede provocar daños físicos, tanto en la impresora como en el edificio donde se encuentre, además de personales.

5.2 Vulnerabilidades

Las impresoras utilizan diferentes protocolos para comunicarse con otros dispositivos. Es habitual que una impresora admita diferentes protocolos para mejorar su compatibilidad con otros sistemas. Estos protocolos son utilizados para ofrecer servicios como FTP, SMB, Web, etc. Podemos encontrar vulnerabilidades en muchos de estos protocolos y servicios, dependiendo del modelo de la impresora y de si está o no actualizada.

Protocolo RAW/AppSocket:

El protocolo RAW/AppSocket se utiliza en algunas impresoras para la impresión de documentos. Este protocolo escucha en el puerto 9100, permitiendo imprimir todo lo que escuche por ese puerto. Por tanto,

si hacemos una petición GET a la impresora por el puerto 9100, ésta imprimirá la petición GET entera. Esto hace que este protocolo sea inseguro por sí mismo, permitiendo la impresión de forma no controlada.

Protocolo SNMP:

El protocolo SNMP (*Simple Network Management Protocol*) es utilizado por la gran mayoría de impresoras para el intercambio de información con otros dispositivos en red.

Este protocolo, no implementa seguridad en la capa de transporte (en sus versiones SNMPv1 y SNMPv2), al no cifrar la información que envía. Esto permite que un atacante pueda capturar el tráfico de la impresora y así robar información privada como las credenciales de acceso... etc. Por tanto, este protocolo es inseguro de por sí en sus versiones v1 y v2. En cambio, la última versión, SNMPv3, sí se considera segura ya que cifra la información enviada.

Además, el uso de los espacios de nombre SNMP por defecto o intuitivos (como "private", "snmp", o usando el nombre del propio fabricante), facilitan al atacante interactuar con la impresora permitiéndole reconfigurar los parámetros TCP/IP, las credenciales, inyectar entradas en la tabla de enrutamiento del dispositivo, etc.

Comandos RSH:

Algunas impresoras permiten la ejecución de comandos RSH, los cuales funcionan a través del protocolo "rlogin". Con estos comandos podemos obtener información sobre la impresora sin necesidad de *loguearnos*. Permite obtener información sobre el estado de la impresora, acceder al log del sistema de la impresora, obtener información sobre documentos impresos (hora y número de páginas) y de los procesos que están corriendo, además de permitir imprimir y reiniciar la impresora.

UPnP:

Aunque UPnP facilita la conexión entre dispositivos, lo encontramos muchas veces activado por defecto, permitiendo imprimir páginas de prueba, resetear la impresora a los ajustes de fábrica, resetear las credenciales de acceso al panel web, o incluso cambiar las configuraciones TCP/IP y de red.

Protocolo SMB:

Cabe mencionar también el protocolo SMB, el cual es frecuentemente implementado por el propio fabricante en sus sistemas Linux o se utilizan versiones antiguas del mismo. Estas versiones e implementaciones son comúnmente vulnerables a ejecución de código remoto. Por ejemplo, recientemente se ha descubierto la vulnerabilidad CVE-2017-7494, la cual permite la ejecución de código remoto en versiones de Samba modernas (versión 3.5.0 en adelante).

Servidor Web:

Las impresoras, al disponer de servidor web para la aplicación de administración de la impresora, pueden tener vulnerabilidades web. Las más comunes están descritas en el OWASP Top 10, y es bastante frecuente encontrarlas presentes en dichas aplicaciones web, puesto que normalmente se diseñan

pensando en el usuario y sin considerar su posible exposición a Internet o a un usuario malicioso en la misma red local.

Además, utilizar el servidor web sin HTTPS permite a un atacante capturar el tráfico de la impresora, obteniendo las credenciales de acceso así como los ficheros enviados a la impresora mediante la plataforma web.

FTP:

Algunas impresoras disponen de servidor FTP para almacenar ficheros o como protocolo de impresión. Se conocen múltiples vulnerabilidades de este servicio que se aprovechan para imprimir documentos sin autenticación, realizar un ataque de denegación de servicio de la impresora o realizar escaneos de red, entre otros.

Vulnerabilidades del sistema operativo:

En muchas ocasiones, las impresoras incorporan sistemas Linux antiguos con vulnerabilidades que permiten escalado de privilegios. Esto, en combinación con otras vulnerabilidades, permite que un atacante explote una vulnerabilidad y escale privilegios en la impresora, tomando el control de la misma para obtener información confidencial, escanear la red interna, capturar tráfico, etc.

Puede suponer un riesgo también el tener servicios ejecutados como root en la impresora, grupos de usuarios mal configurados o permisos de ficheros mal configurados, permitiendo a un atacante ganar privilegios en la impresora y comprometerla.

Una impresora comprometida puede suponer el acceso a las contraseñas almacenadas en ella, puesto que en muchas de ellas se almacenan en claro en ficheros de configuración.

5.3 Consejos y recomendaciones de uso y configuración

Los usuarios de impresoras pueden ayudar a contener las amenazas potenciales que plantea la conectividad de red y ponderar los riesgos de un agujero o fallo de seguridad del dispositivo, considerando la necesidad de conexión.

El llevar a cabo unas recomendaciones básicas de seguridad conlleva a unas buenas prácticas que los usuarios deben tener en cuenta a la hora de la conexión de sus dispositivos.

A continuación destacamos las siguientes recomendaciones:

- Utilizar las funcionalidades de seguridad tales como la impresión segura con PIN, autenticación por LDAP, smart cards, identificación por RFID o con sensores biométricos. En caso de que no se puedan implementar controles técnicos, concienciar a los usuarios en la recogida inmediata del documento impreso.

- Modificar la contraseñas por defecto (de acceso a la interfaz web de la impresora,...).
- Utilizar contraseñas robustas, que dificulten los posibles ataques de fuerza bruta.
- Evitar configurar usuarios en la impresora que dispongan de privilegios en la red corporativa. Si roban las credenciales en la impresora que no puedan acceder a ningún otro servicio.
- Utilizar conexiones cifradas con la impresora siempre que sea posible.
- Si la impresora lo permite, borrar los documentos de la impresora después de imprimirlos y/o escanearlos.
- No exponer las impresoras a Internet.
- Securizar las impresoras en la red local:
  - Considerar el aislamiento de las impresoras, dejándolas en una red controlada a parte.
  - Configurar listas de control de acceso (ACL - Access Control List) para restringir el acceso a la impresora a nivel de red.
  - Configurar una máquina como servidor de impresión la cual implemente controles de acceso y medidas de seguridad.
- Si se dispone de herramientas de monitorización de red, es conveniente configurar reglas que detecten cualquier actividad inusual sobre la impresora.
- Desactivar los protocolos y servicios no utilizados (FTP, SSH, Telnet, Wi-Fi...): Si se dejan dichos servicios activos se corre el riesgo de que un atacante pueda acceder a datos e información de la impresora directamente, permitiendo incluso el acceso a los datos almacenados en el disco duro de la impresora.
- Utilizar Ethernet antes que Wi-Fi o Bluetooth: Las impresoras que disponen de conectividad inalámbrica casi siempre también ofrecen conectividad por Ethernet. Es recomendable utilizar Ethernet antes que Wi-Fi o Bluetooth puesto que el medio no es compartido. También es recomendable desactivar las conexiones inalámbricas cuando no se utilicen.
- Realizar un estudio del nivel de seguridad de las impresoras antes de adquirirlas.
- Actualizar y parchear: Las impresoras también necesitan ser actualizadas. Los fabricantes parchean tanto problemas de funcionamiento como de seguridad. Por ello, es recomendable comprobar las actualizaciones de Firmware de forma regular y descargarlas siempre de la página del fabricante.
- A la hora de deshacerse de una impresora se deben borrar todos los datos personales y confidenciales del disco duro. Para ello se debe de contactar primero con el fabricante para preguntar si disponen de alguna herramienta que haga un borrado seguro de toda la información de la impresora, haciendo que los datos personales y confidenciales sean imposibles de recuperar. En caso de que el fabricante no disponga de ninguna herramienta para tal fin se deberá considerar el extraer el disco duro de la impresora y realizar un borrado seguro del mismo. No obstante, algunas

impresoras tienen discos duros no extraíbles, en cuyo caso se recomienda localizar y destruir físicamente el disco duro.

6 CONCLUSIONES

Las impresoras son elementos de nuestra red muchas veces ignorados en cuanto a seguridad se refiere. La seguridad es un concepto que se debe aplicar durante toda la vida útil de las impresoras: desde su creación hasta el momento en el que nos deshacemos de ella.

Los vectores de ataque de las impresoras son variados y permiten desde el robo de información confidencial, comprometer toda nuestra red y otros servicios internos, hasta provocar daños físicos en la impresora y en las oficinas.

Los fabricantes de impresoras multifunción tienen la responsabilidad de incluir la seguridad desde la fase de diseño. Aunque se aprecia una evolución en las medidas de seguridad que muchos fabricantes aplican a sus impresoras, se observa que aún no es algo generalizado. Por lo que se debe prestar atención a este aspecto en el momento de la adquisición.

Se deben implementar medidas que contrarresten las carencias de seguridad que las impresoras traen de fábrica. Además, debemos tener en cuenta que hay impresoras multifunción antiguas en funcionamiento, las cuales fueron diseñadas en un momento en el cual la seguridad no era una prioridad o incluso no se tenía en cuenta. Por ello, se debe de aplicar medidas de seguridad extra a este tipo de impresoras, las cuales utilizan protocolos inseguros o tienen vulnerabilidades en sus sistemas.

7 GLOSARIO

FTP: (Protocolo de transferencia de datos) Protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor.

SNMP: El Protocolo Simple de Administración de Red o SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Versión actual SNMPv3.

RFID: Identificación por radiofrecuencia (del inglés Radio Frequency Identification) es un sistema de almacenamiento y recuperación de datos remoto que usa dispositivos denominados etiquetas, tarjetas o transpondedores RFID.

8 DOCUMENTACION DE REFERENCIA

- [1] Hack en impresora permite ejecutar el juego Doom:
  https://www.wired.com/2014/09/doom-printer/
- [2] Prueba de concepto de ataque a impresoras generando daños físicos:
  http://www.nbcnews.com/business/consumer/exclusive-millions-printers-open-devastating-hack-attack-researchers-say-f118851
- [3] Vulnerabilidad en impresoras HP JetDirect que permiten acceso a cualquier usuario:
  http://securitytracker.com/id/1006641
- [4] Vulnerabilidad CVE-2007-1772 que genera una denegación de servicio en impresoras HP:
  http://www.cvedetails.com/cve/CVE-2007-1772/
- [5] Certificado NAPS de ICSA para la seguridad en dispositivos en red:
  https://www.icsalabs.com/technology-program/network-attached-peripherals
- [6] La amenaza oculta en las impresoras multifunción:
  https://www.forbes.com/sites/ciocentral/2013/02/07/the-hidden-it-security-threat-multifunction-printers/#73cf373b615a
- Seguridad en el protocolo SNMP:
  https://principiatechnologica.com/2013/06/18/snmpv2-usa-snmpv3/
- Hacking de impresoras:
  http://archive.hack.lu/2010/Costin-HackingPrintersForFunAndProfit-slides.pdf
- Evolución de las impresoras multifunción:
  http://historia-y-evolucion-de-la-impresora.blogspot.com.es/
- Vulnerabilidad FTP en impresoras Dell:
  https://isc.sans.edu/forums/diary/Printer+Hacking+for+Fun+and+Profit/1637/
- Todo lo que necesitas saber sobre seguridad en impresoras:
  http://www.notebookreview.com/feature/everything-you-need-to-know-about-printer-security/
- Buenas prácticas para la utilización de estas impresoras:
  https://security.berkeley.edu/resources/best-practices-how-articles/network-printer-security-best-practices
- Hacking de impresoras:
  http://www.irongeek.com/i.php?page=security/networkprinterhacking
- La seguridad de las impresoras también importa:
  https://www.securityartwork.es/2017/02/06/printesting-la-seguridad-las-impresoras-tambien-importa/
- Hacking Ético: Seguridad en las impresoras:
  https://hacking-etico.com/2016/04/21/seguridad-las-impresoras/
- ¿Supone tu impresora un riesgo de seguridad?:
  http://securitywatch.pcmag.com/vulnerabilities/283948-is-your-home-printer-a-security-risk

- Buenas prácticas para la securización de las impresoras:
  http://www.networkworld.com/article/2190118/lan-wan/best-practices-for-printer-security.html
- Atacando una impresora de oficina:
  https://security.stackexchange.com/questions/23691/attacking-an-office-printer
- Las impresoras como el próximo vector de ataque:
  https://it.slashdot.org/story/11/11/29/1752231/printers-could-be-the-next-attack-vector