Se han descubierto vulnerabilidades de seguridad en las impresoras multifuncionales Xerox VersaLink C7025 (MFP), las cuales podrían permitir a los atacantes capturar credenciales de autenticación mediante ataques de tipo pass-back aprovechando los protocolos LDAP (Protocolo Ligero de Acceso a Directorios) y los servicios SMB/FTP.

> *«Este ataque de tipo pass-back explota una vulnerabilidad que permite a un actor malicioso modificar la configuración de la impresora multifuncional y hacer que el dispositivo envíe las credenciales de autenticación de vuelta al atacante»*, explicó Deral Heiland, investigador de seguridad de Rapid7.
>
> *«Si un atacante logra aprovechar estos problemas con éxito, podría capturar credenciales de Windows Active Directory. Esto les permitiría moverse lateralmente dentro de la red de una organización y comprometer otros servidores y sistemas de archivos críticos de Windows».*

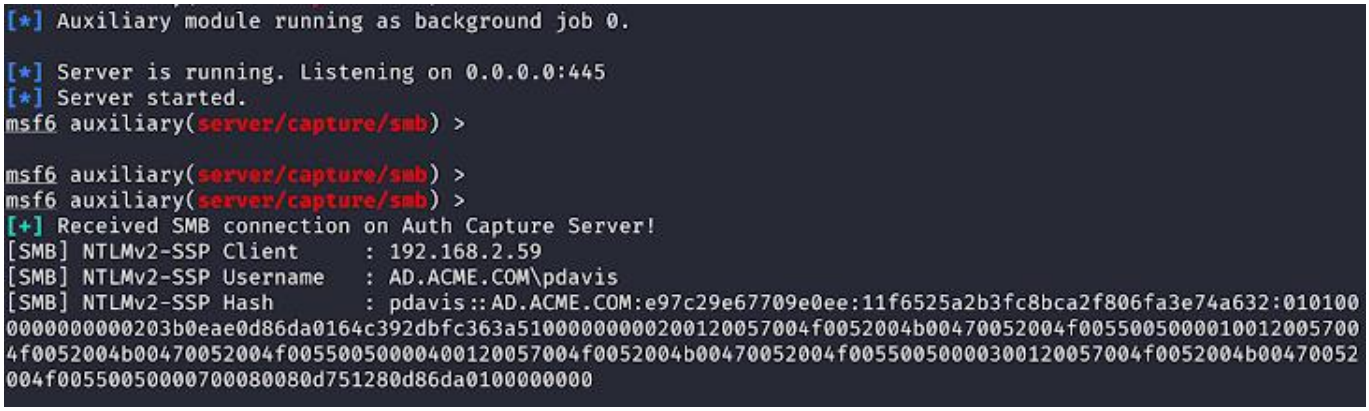
Las vulnerabilidades identificadas, que afectan a versiones de firmware 57.69.91 y anteriores, son las siguientes:

- CVE-2024-12510 (puntuación CVSS: 6.7) – Ataque pass-back a través de LDAP
- CVE-2024-12511 (puntuación CVSS: 7.6) – Ataque pass-back a través de la libreta de direcciones del usuario

La explotación exitosa de CVE-2024-12510 podría permitir que la información de autenticación se redirija a un servidor malicioso, lo que expondría las credenciales. Sin embargo, esto requeriría que el atacante tuviera acceso a la página de configuración LDAP y que LDAP se estuviera utilizando para la autenticación.

Por otro lado, CVE-2024-12511 permite a un atacante obtener acceso a la libreta de direcciones del usuario y modificar la dirección IP del servidor SMB o FTP, redirigiéndola hacia un servidor bajo su control. Esto provocaría que las credenciales de autenticación SMB o FTP

sean capturadas durante las operaciones de escaneo de documentos.



> *«Para que este ataque sea efectivo, el atacante debe haber configurado una función de escaneo SMB o FTP dentro de la libreta de direcciones del usuario y tener acceso físico a la consola de la impresora o acceso remoto mediante la interfaz web. Esto puede requerir privilegios de administrador, a menos que se haya habilitado el acceso a la consola remota para usuarios con privilegios más bajos»,* comentó Heiland.

Después de la divulgación responsable de las vulnerabilidades el 26 de marzo de 2024, estas fueron solucionadas en el Service Pack 57.75.53, que se lanzó a finales del mes pasado para las impresoras VersaLink C7020, 7025 y 7030.

Si no se puede aplicar un parche inmediato, se recomienda a los usuarios establecer contraseñas complejas para la cuenta de administrador, evitar el uso de cuentas de autenticación de Windows con privilegios elevados y deshabilitar el acceso a la consola remota para usuarios no autenticados.

Esta situación surge mientras Peyton Smith, fundador y CEO de Specular, reveló una vulnerabilidad de inyección SQL no autenticada que afecta a un software ampliamente utilizado en el sector salud, HealthStream MSOW (CVE-2024-56735). Esta vulnerabilidad

podría permitir el acceso total a la base de datos, lo que permitiría a los atacantes obtener información sensible de 23 organizaciones de salud a través de internet.

La empresa indicó que identificó 50 instancias de MSOW expuestas en internet, de las cuales 23 presentan fallos de seguridad que las hacen vulnerables.

La vulnerabilidad podría permitir que *«toda la base de datos se devuelva dentro de la misma transmisión, lo que significa que un atacante podría obtener el contenido en texto claro de la base de datos a través de una respuesta HTTP generada por una inyección SQL diseñada»*, explicó Smith.