Se ha descubierto una forma para abusar de la tecnología conocida como enlaces *«mailto»* para lanzar ataques a los usuarios de clientes de escritorio de correo electrónico.

Los nuevos ataques pueden usarse para robar de forma secreta archivos locales y enviarlos por correo electrónico como archivos adjuntos a los atacantes, según un artículo publicado la semana pasada por académicos de dos universidades alemanas.

La vulnerabilidad reside en la forma como los clientes de correo electrónico implementaron RFC6068, el estándar técnico que describe el esquema de URI «mailto».

Mailto hace referencia a tipos especiales de enlaces, que generalmente son compatibles con navegadores web o clientes de correo electrónico. Estos son enlaces que, al darles clic, abren una nueva ventana de redacción/respuesta de correo electrónico en lugar de una nueva página web.

RFC6068 especifica que los enlaces mailto pueden admitir varios parámetros. Cuando se utiliza con enlaces de correo electrónico, estos parámetros rellenarán previamente la nueva ventana de correo electrónico con contenido predefinido.

Por ejemplo, un vínculo mailto como el que se muestra abajo, abrirá una nueva ventana de redacción de correo electrónico con el correo de destino ya completado, una línea de asunto y un texto de correo electrónico.

```
<a href="mailto:bob@host.com? Subject=Hello& body=Friend">
¡Haz clic aquí! </a>
```

El estándar RFC6068 (mailto) admite un gran conjunto de parámetros para personalizar los enlaces mailto, incluidas las opciones que se utilizan con poca frecuencia y que se pueden utilizar para controlar el texto del cuerpo del correo electrónico, la dirección de correo de

respuesta e incluso los encabezados de correo electrónico.

Sin embargo, el propio estándar advierte a los ingenieros de software que no admitan todos los parámetros, recomendando que las aplicaciones solo admitan algunas opciones seguras.

Algunos clientes de correo electrónico admitían parámetros peligrosos de mailto

En el artículo titulado «*Mailto: Me Your Secrets*«, los investigadores de la Universidad de Ruhr en Bochum y la Universidad de Ciencias Aplicadas de Münster, dijeron que encontraron aplicaciones de cliente de correo electrónico que admiten el estándar mailto con algunos de sus parámetros *«más exóticos»* que permiten ataques a sus usuarios.

Particularmente, los investigadores observaron los parámetros de *«adjuntar»* de mailto que permiten que los enlaces abran nuevas ventanas de redacción/respuesta de correo electrónico con un archivo ya adjunto.

Los académicos dicen que los atacantes pueden enviar correos electrónicos que contengan enlaces mailto con trampas maliciosas, o colocar enlaces mailto con trampa maliciosa en sitios web que, al hacer clic en ellos, podrían adjuntar archivos confidenciales a la ventana de correo electrónico.

Si el usuario que redacta el correo electrónico no detecta el archivo adjunto, los atacantes podrían recibir archivos confidenciales del sistema del usuario, como claves de cifrado (PGP), claves SSH, archivos de configuración, archivos de billetera de criptomonedas, almacenes de contraseñas o documentos comerciales importantes, siempre que estén almacenados en rutas de archivo conocidas por un atacante.

Los investigadores agregaron que probaron varias versiones de la técnica de exfiltración de datos, como:

- Utilizar rutas exactas para los archivos deseados
- Usar caracteres comodín (*) para adjuntar/robar varios archivos a la vez
- Uso de URL para recursos compartidos de la red interna (\dominio_empresa\archivo)
- Usar la URL que dirija a la víctima al servidor SMB malicioso de un atacante, por lo que la víctima filtra su hash de autenticación NTLM al atacante (\evil.com\dummyfile)
- Uso de enlaces IMAP para robar mensajes de correo electrónico de toda la bandeja de entrada de correo IMAP de un usuario (imap:\\fetch>UID>INBOX)

El equipo de investigadores dijo que probó 20 clientes de correo electrónico para su escenario de ataque y descubrió que cuatro clientes eran vulnerables. La lista incluye:

- Evolution: El cliente de correo electrónico predeterminado para el entorno de escritorio GNOME en Linux (CVE-2020-11879)
- KMail: El cliente de correo electrónico predeterminado para entornos de escritorio KDE en Linux (CVE-2020-11880)
- IBM/HCL Notes en Windows (CVE-2020-4089)
- Versiones anteriores de Thunderbird en Linux (ahora parcheadas)

Todos los problemas encontrados fueron informados a los respectivos equipos de desarrollo y se corrigieron este año.

Ataques PGP y S/MIME cifrados

Además, el artículo también describe errores en los clientes de correo electrónico que pudieron ser abusados para eludir tecnologías de encriptación de correo electrónico como PGP y S/MIME.

Los investigadores tuvieron éxito al encontrar tres nuevas técnicas de ataque que aprovecharon los errores en los clientes de correo electrónico para robar las claves privadas PGP de las víctimas, lo que permitiría a los atacantes descifrar todas las comunicaciones de la víctima.

Las tres nuevas clases de ataques se enumeran a continuación:

1.- Reemplazo de clave: Los clientes de correo electrónico pueden instalar automáticamente los certificados contenidos en las comunicaciones S/MIME. Esta función, de estar disponible, se puede utilizar de forma incorrecta para reemplazar silenciosamente la clave pública utilizada para cifrar mensajes a una determinada entidad.

2.- Oráculos DEC/SIG: Utilizando parámetros estándar de mailto, los clientes de correo electrónico pueden ser engañados para que descifren mensajes de texto cifrado o firmen mensajes arbitrarios, y exfiltrarlos a un servidor IMAP controlado por el atacante, si el cliente de correo electrónico admite guardar borradores de mensajes automáticamente.

3.- Exfiltración de claves: Si lo implementa el cliente de correo electrónico, un atacante puede crear un esquema de URI mailto especialmente diseñado para forzar la inclusión del archivo de clave privada OpenPGP en el disco en un correo electrónico que se enviará al atacante.

Los investigadores dijeron que ocho de los 20 clientes de correo electrónico que probaron para su proyecto de investigación, eran vulnerables a al menos uno de los tres ataques enumerados anteriormente.