BOLETÍN DE ALERTA

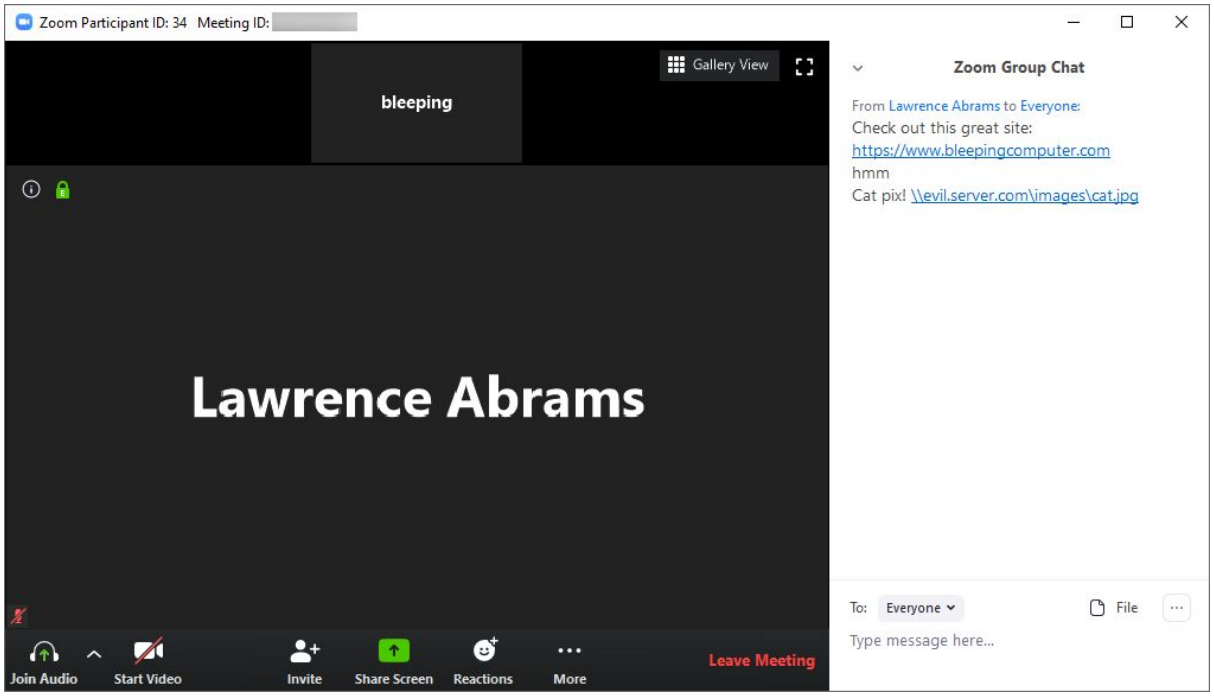
Boletín Nro.: 2020-10
Fecha de publicación: 02/04/2020
Tema: Vulnerabilidad en Zoom permitiría a un atacante remoto obtener las credenciales de acceso de Windows.

Sistemas afectados:

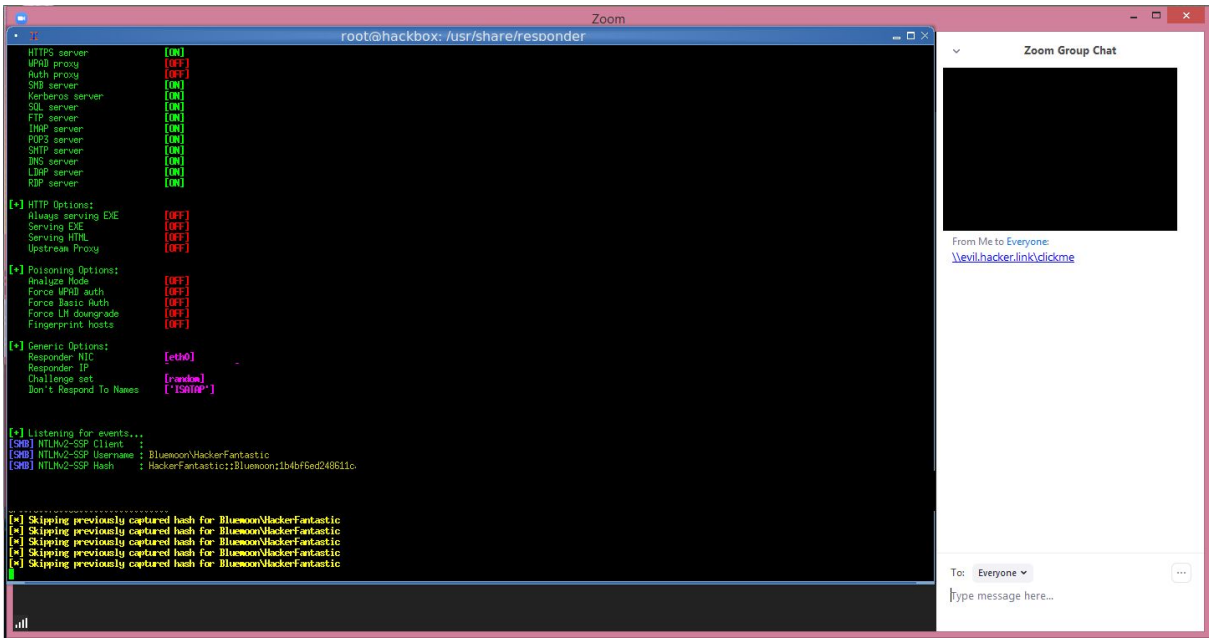
- Zoom para Windows en todas sus versiones.

Descripción:

Recientemente se ha descubierto una falla en el cliente de **Zoom** para Windows, concretamente una vulnerabilidad de inyección de **ruta UNC** en la funcionalidad de **chat**.
Zoom por defecto convierte todas las **URLs** que son compartidas en el chat en **hipervínculos** para que de esta manera los participantes de la reunión puedan hacer clic en él e ir directamente a la página web indicada en la **URL**. Pero además de esto, **Zoom** también convierte las **rutas UNC de red de Windows** para acceder a un recurso remoto desde el chat, con lo que al hacer clic sobre él se intentará una conexión a través del protocolo **SMB**.
Un atacante remoto podría aprovechar esta situación, enviar a través del chat una **URL** especialmente diseñada y convencer a la víctima que haga clic en el mismo.



Cuando esto ocurre Windows intentará conectarse al sitio remoto utilizando el protocolo **SMB**, que de forma predeterminada enviará el nombre de inicio de sesión del usuario y el **hash** de contraseña **NTLM**, el cual puede ser capturado por el atacante.



Si bien esta contraseña no es capturada en texto plano, puede utilizarse herramientas como john the ripper o hashcat para intentar descifrar la contraseña, si la misma es una contraseña débil, sólo tomará un par de segundos descifrarla. En cambio en un ambiente corporativo, el nombre de usuario y el **hash** puede ser utilizado para acceder a otros equipos y obtener otros vectores de ataque.

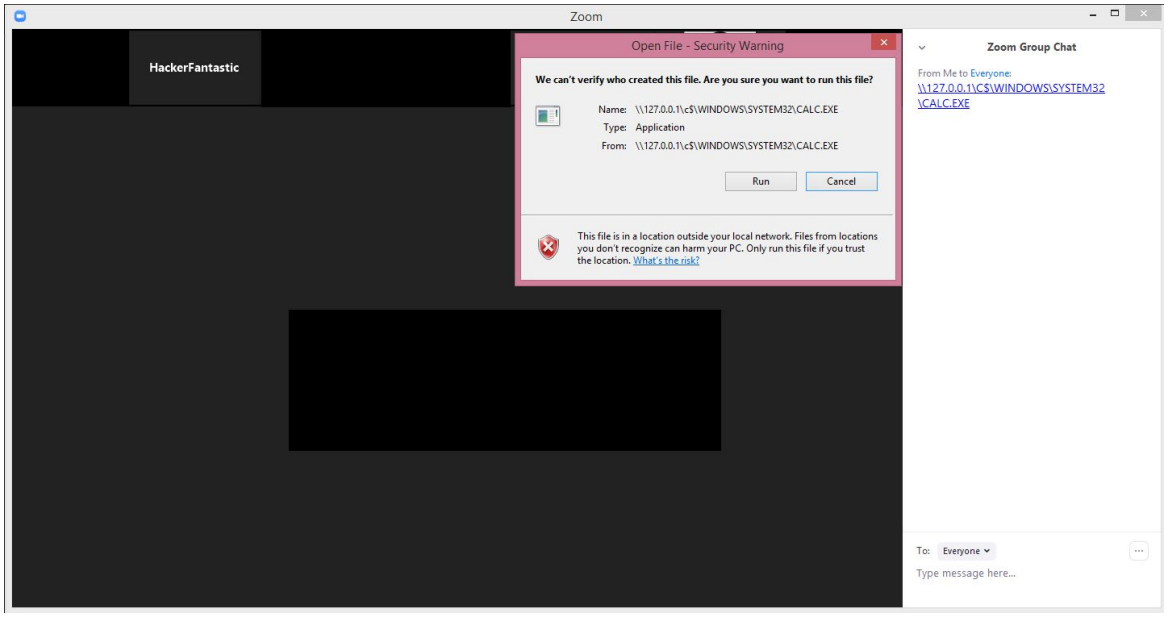
```
Cache-hit dictionary stats ..\hashkiller-dict.txt: 588725864 bytes, 47625548 words, 47625548 keyspace

SECTEST1233@OUTLOOK.COM::MicrosoftAccount:1122334455667788:0e5394410a4c4f935493ffa89a3cdd85:0101000000000001483812 87aeed1012d77818c
cccee1f900000000020034006d0073006c0065006100 6b002e0070006500720066006500630074002d0070007200690076006100630079002e0063006f006d000000
000000000000:newyork11

Session.Name...: hashcat
Status.........: Cracked
Input.Mode.....: File (..\hashkiller-dict.txt)
Hash.Target....: SECTEST1233@OUTLOOK.COM::MicrosoftAccount...
Hash.Type......: NetNTLMv2
Time.Started...: Thu Aug 04 14:06:00 2016 (3 secs)
Speed.Dev.#2...:  5521.7 kH/s (12.41ms)
Recovered......: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.......: 17254121/47625548 (36.23%)
Rejected.......: 706793/17254121 (4.10%)
Restore.Point..: 16294344/47625548 (34.21%)

Started: Thu Aug 04 14:06:00 2016
Stopped: Thu Aug 04 14:06:14 2016
```

Además, un atacante remoto podría ejecutar cualquier software que se encuentre en el equipo o realizar la descargar de código malicioso en el mismo.



Un ejemplo de explotación de esta vulnerabilidad lo puede ver en el siguiente enlace.

Por otro lado, no es el único fallo de seguridad o privacidad que se ha descubierto en **Zoom,** existen varios reportes los cuales mencionan que otros usuarios ajenos a una reunión han logrado **"piratear"** la reunión, acceder a la misma y exhibir imágenes pornográficas o racistas en las pantallas durante las reuniones, por lo que se solicita extremar las precauciones con el fin realizar una reunión segura.

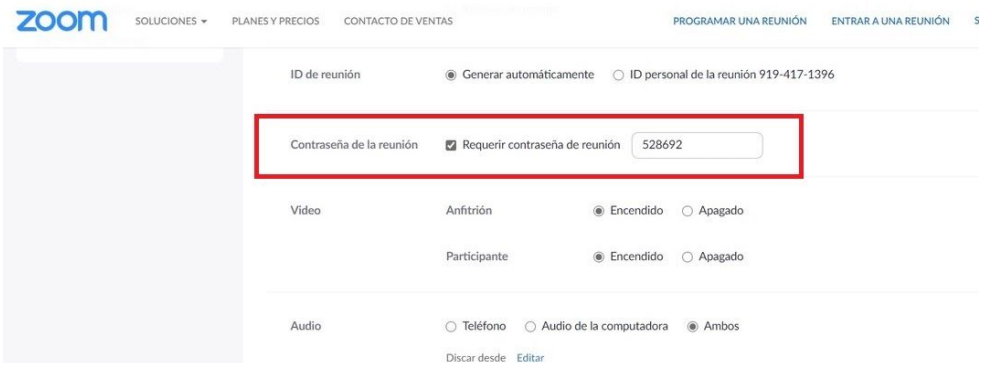
Impacto:

Esta vulnerabilidad podría permitir a un atacante remoto obtener las credenciales de acceso de un usuario de Windows, además ejecutar cualquier software que se encuentre en el equipo o realizar la descargar de código malicioso en el mismo.0

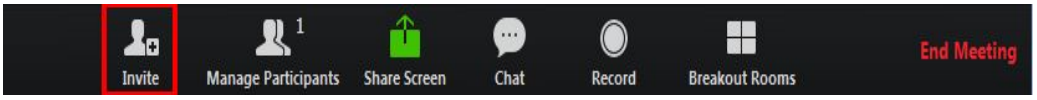
Solución y prevención:

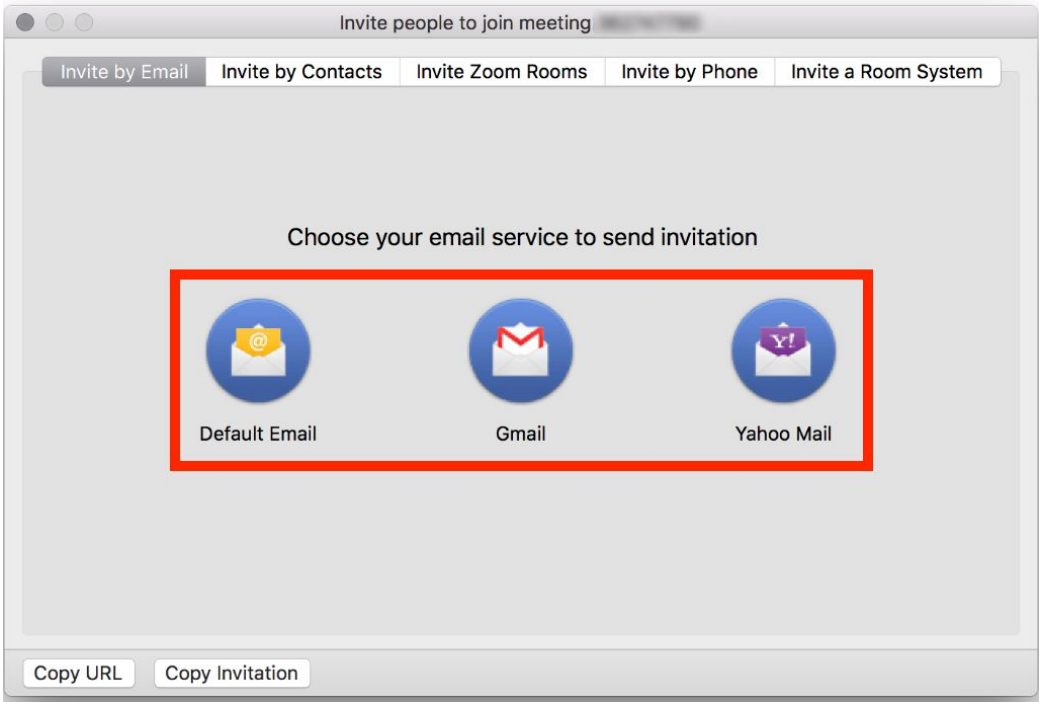
- Aún no existen parches de seguridad que abordan esta vulnerabilidad, por lo que se recomienda utilizar un software de videoconferencia alternativo o **Zoom** en la versión del navegador.
- Para realizar una reunión segura, se recomienda que siga las siguientes indicaciones:

- No haga pública las reuniones o aulas, **Zoom** cuenta con la opción de hacer que una reunión sea privada o de ingresar una contraseña para unirse a la misma.

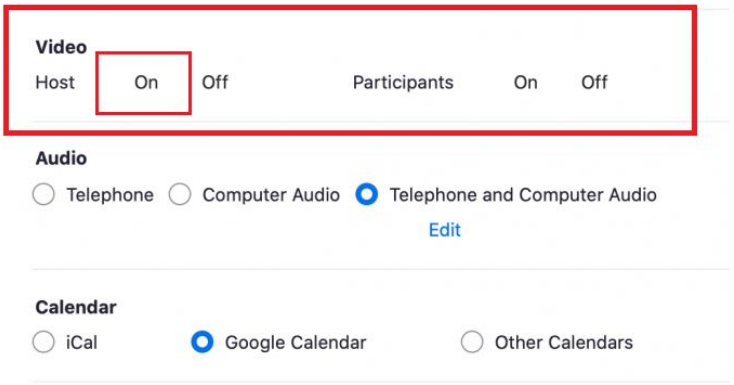


- No comparta el enlace a una reunión a través de las redes sociales. Es más seguro enviar el enlace directamente a las personas con quien se acuerde la reunión.

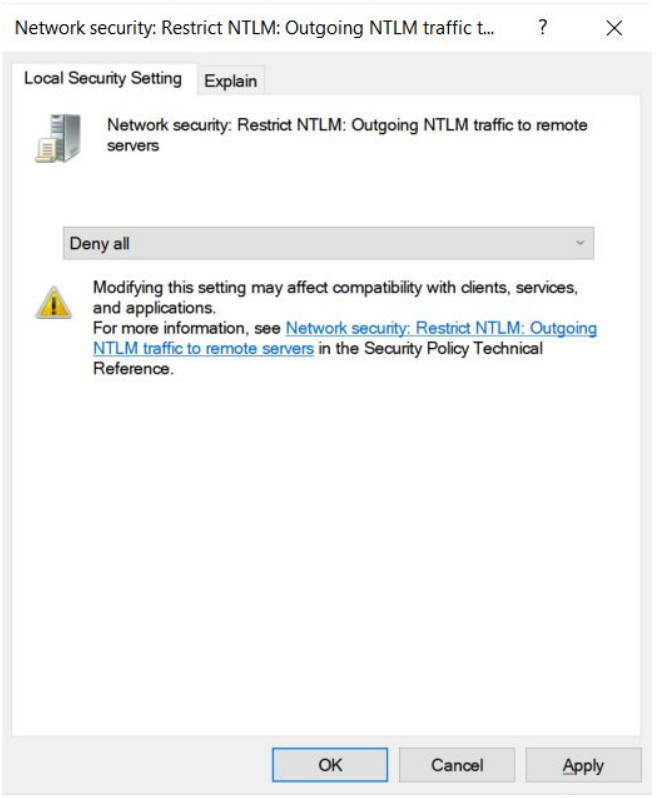




- Cambie el uso compartido de la pantalla a **"Solo host"**.

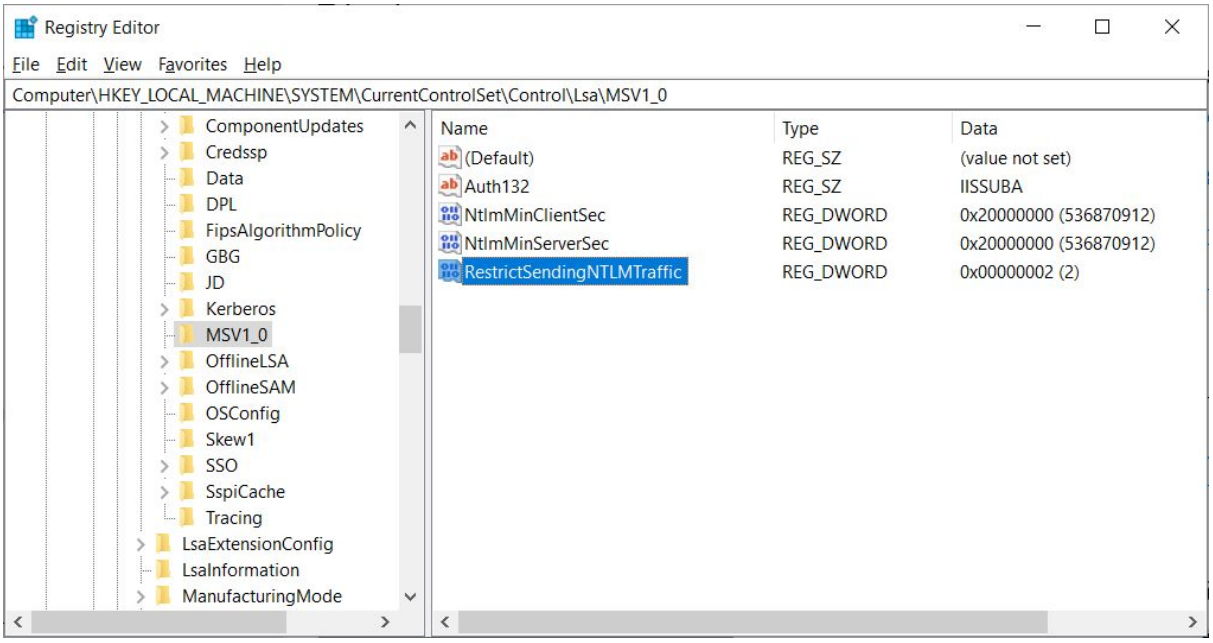


- Para equipos pertenecientes a un dominio, cambiar la configuración de la política de seguridad para restringir que el sistema operativo pase automáticamente sus credenciales **NTML** a un servidor remoto, para ello diríjase a:
    - **Configuración del equipo > Configuración de Windows > Configuración de seguridad > Directivas locales > Opciones de seguridad > Red de seguridad: Restringir NTLM: NTLM tráfico saliente a servidores remotos.**
    - y configure la política en **deny all**.



- Tambíen es posible cambiar la política desde el editor de registro de Windows ***(Tenga en cuenta que una mala configuración en los registro podría dañar el mismo)***:
    - Inicie el editor del registro como administrador.
    - Cree el valor **RestrictSendingNTLMTraffic** en la clave **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0**. y
    - asigne número 2 en el campo de **Value Data**.

Para ver un vídeo explicativo de la configuración del registro, puede dirigirse al siguiente enlace.



Información adicional:

- https://www.bleepingcomputer.com/news/security/zoom-lets-attackers-steal-windows-credentials-via-unc-links/
- https://thehackernews.com/2020/04/zoom-windows-password.html
- https://mashable.com/article/zoom-vulnerability-windows-passwords/
- https://m.excelsior.com.mx/hacker/zoom-en-la-mira-del-fbi-por-hackeo-durante-videoconferencias/1373244