Evidencia y Analisis de Vulnerabilidad

Configuracion insegura de FTP (vsftpd) en Debian

Fecha del informe: 08 enero 2026

Resumen ejecutivo

Se identifico una configuracion insegura del servicio FTP (vsftpd) que puede exponer archivos y credenciales, y ampliar la superficie de ataque del servidor. La evidencia proviene de la revision de la configuracion (/etc/vsftpd.conf), controles de acceso (/etc/ftpusers) y permisos del directorio FTP (/srv/ftp).

Hallazgo	Evidencia	Riesgo/Impacto
Acceso anonimo habilitado	anonymous_enable=YES	Permite acceso sin cuenta; posible exposicion de archivos y reconocimiento del servicio.
Login de usuarios locales habilitado	local_enable=YES	Habilita autenticacion de cuentas del sistema; riesgo de fuerza bruta/credenciales reutilizadas.
Escritura habilitada (global)	write_enable=YES	Si existen permisos de escritura en directorios FTP, permite carga/modificacion de archivos (persistencia, DoS, alteracion).
Sin aislamiento por chroot	chroot_local_user no activo	Usuarios FTP locales no quedan forzados a su HOME; pueden navegar donde el sistema lo permita (exfiltracion).
Sin cifrado (FTP en texto plano)	ssl_enable=NO	Credenciales y datos viajan sin cifrar; riesgo de sniffing/MITM en la red.

Evidencia recolectada

1) Estado del servicio y exposicion del puerto

Comando recomendado para ver el servicio escuchando en el puerto 21:

```
sudo ss -tulpn | grep -E '(:21)\b'
```

Observacion del entorno: vsftpd se encuentra escuchando en el puerto 21 (FTP). Si escucha en 0.0.0.0:21 o *:21, el servicio queda accesible desde la red y no solo desde localhost.

2) Configuracion de vsftpd

Salida obtenida al revisar parametros criticos en /etc/vsftpd.conf:

```
sudo grep -nE "anonymous_enable|local_enable|write_enable|anon_upload_enable|" \
  -e "anon_mkdir_write_enable|anon_other_write_enable|chroot_local_user|allow_writeable_chroot" \
```

```
  -e "userlist_enable|userlist_deny|ssl_enable|force_local_logins_ssl|force_local_data_ssl" \
  /etc/vsftpd.conf
25:anonymous_enable=YES
28:local_enable=YES
31:write_enable=YES
40:#anon_upload_enable=YES
44:#anon_mkdir_write_enable=YES
114:#chroot_local_user=YES
122:#chroot_local_user=YES
151:ssl_enable=NO
```

3) Controles de acceso del sistema

Archivo /etc/ftpusers (usuarios a los que se les niega acceso por FTP):

```
sudo cat /etc/ftpusers
# /etc/ftpusers: list of users disallowed FTP access. See ftpusers(5).

root
daemon
bin
sys
sync
games
man
lp
mail
news
uucp
nobody
```

Interpretacion: root y cuentas de sistema (daemon, bin, nobody, etc.) estan bloqueadas para FTP. Esto es positivo, pero no elimina el riesgo asociado a local_enable=YES para usuarios normales.

4) Permisos del directorio FTP

Permisos observados en /srv/ftp:

```
ls -ld /srv/ftp
drwxr-xr-x 2 root ftp 4096 Oct  8  2024 /srv/ftp
```

Interpretacion (755): el propietario (root) puede escribir; el grupo (ftp) y otros solo leen/ejecutan. Esto sugiere que, por defecto, el anonimo no puede subir archivos a /srv/ftp, pero si hay contenido legible por 'otros', puede ser listado/descargado cuando anonymous_enable=YES.

Analisis de riesgos

Confidencialidad: ssl_enable=NO implica credenciales y datos en texto plano. Un atacante en la misma red puede capturar USER/PASS y reutilizarlas. Ademas, anonymous_enable=YES puede permitir listar/descargar archivos publicos en /srv/ftp.

Integridad: write_enable=YES habilita operaciones de escritura. Si algun directorio FTP queda con permisos de escritura para el usuario/grupo correcto, un atacante autenticado podria modificar o introducir archivos no autorizados.

Disponibilidad: el servicio expuesto por red puede ser objetivo de fuerza bruta, saturacion de conexiones o llenado de disco (si existiera escritura en algun punto), provocando degradacion o caida del servicio.

Causas raiz

La combinacion de acceso anonimo, autenticacion de usuarios locales, escritura habilitada y falta de cifrado crea un escenario de alto riesgo. Adicionalmente, la falta de chroot para usuarios locales incrementa la exposicion a directorios fuera del HOME dependiendo de permisos del sistema.

Recomendaciones de correccion y endurecimiento

- Deshabilitar acceso anónimo si no es estrictamente necesario: anonymous_enable=NO.

- Habilitar cifrado TLS (FTPS) y forzarlo para credenciales y datos: ssl_enable=YES, force_local_logins_ssl=YES, force_local_data_ssl=YES; configurar certificados.

- Aplicar aislamiento por chroot para usuarios locales: chroot_local_user=YES (y revisar allow_writeable_chroot si se requiere).

- Reducir superficie: si no se requiere FTP para usuarios locales, poner local_enable=NO. Si se requiere, crear usuarios dedicados y sin shell.

- Restringir quién puede usar FTP con lista: userlist_enable=YES y usar allowlist (userlist_deny=NO) con /etc/vsftpd.user_list.

- Minimizar escritura: mantener write_enable=NO salvo que sea imprescindible; si se habilita, limitarla a un subdirectorio con permisos controlados (ej. 750/770) y propiedad adecuada.

- Auditoría y protección: habilitar logs, limitar conexiones, y considerar fail2ban; filtrar el acceso al puerto 21 por firewall (solo redes necesarias).

- Si el objetivo es transferencia segura, considerar SFTP (sobre SSH) en lugar de FTP/FTPS.

Ejemplo de configuracion recomendada (orientativa)

```
# Endurecimiento básico (ajustar al caso de uso)
anonymous_enable=NO
local_enable=YES
write_enable=NO
chroot_local_user=YES

ssl_enable=YES
```

```
force_local_logins_ssl=YES
force_local_data_ssl=YES

userlist_enable=YES
userlist_deny=NO
# userlist_file=/etc/vsftpd.user_list
```

Validacion posterior (comandos)

```
# Verificar puerto
sudo ss -tulpn | grep -E '(:21)\b'

# Verificar configuracion efectiva
sudo grep -nE "anonymous_enable|local_enable|write_enable|chroot_local_user|ssl_enable" \
  -e "force_local_logins_ssl|force_local_data_ssl|userlist_enable|userlist_deny" \
  /etc/vsftpd.conf

# Probar que NO permite anonymous
ftp <IP_SERVIDOR>  # user: anonymous (debe fallar o limitarse segun diseno)

# Verificar permisos del directorio FTP
ls -ld /srv/ftp
ls -la /srv/ftp
```

Conclusion

Con base en la evidencia revisada, el servidor FTP presenta configuraciones que permiten accesos inseguros y exposicion de informacion. La prioridad inmediata es eliminar el acceso anonimo si no es requerido y habilitar/forzar cifrado TLS (o migrar a SFTP), junto con aislamiento chroot y controles estrictos de usuarios y permisos.