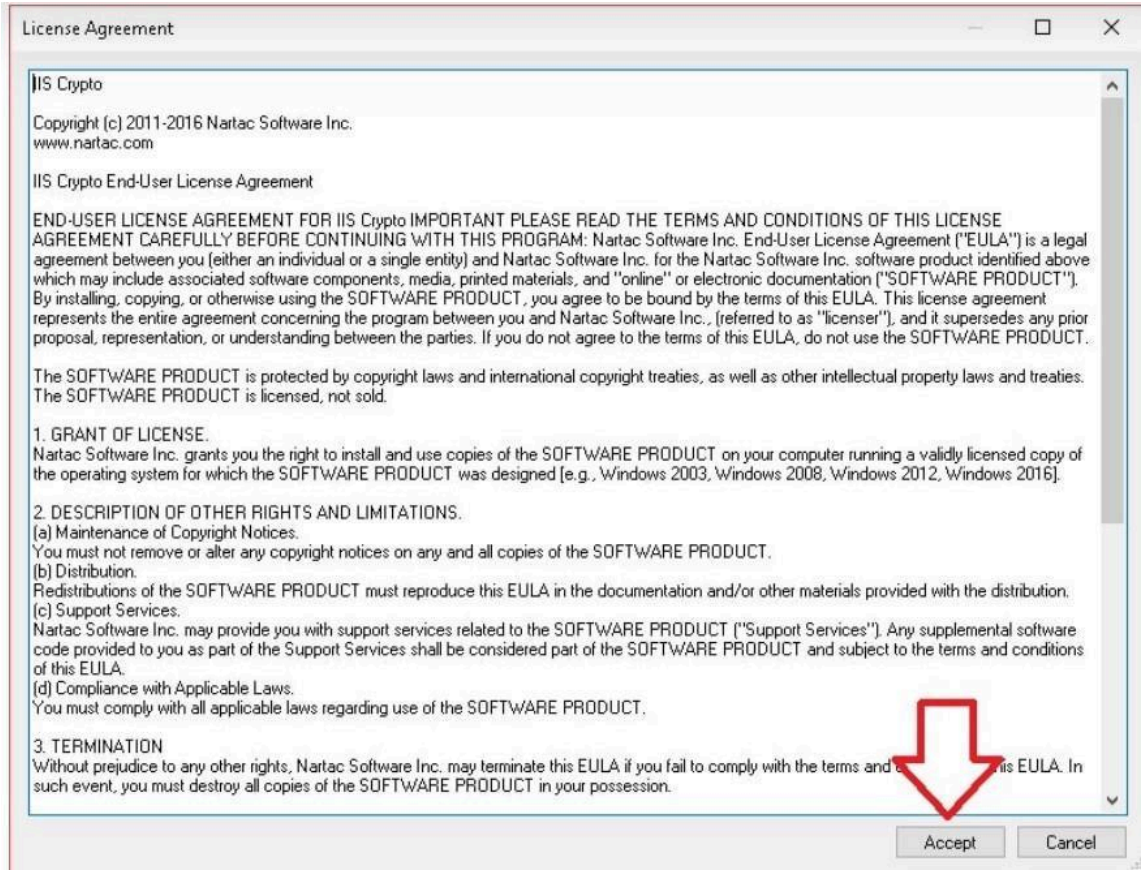
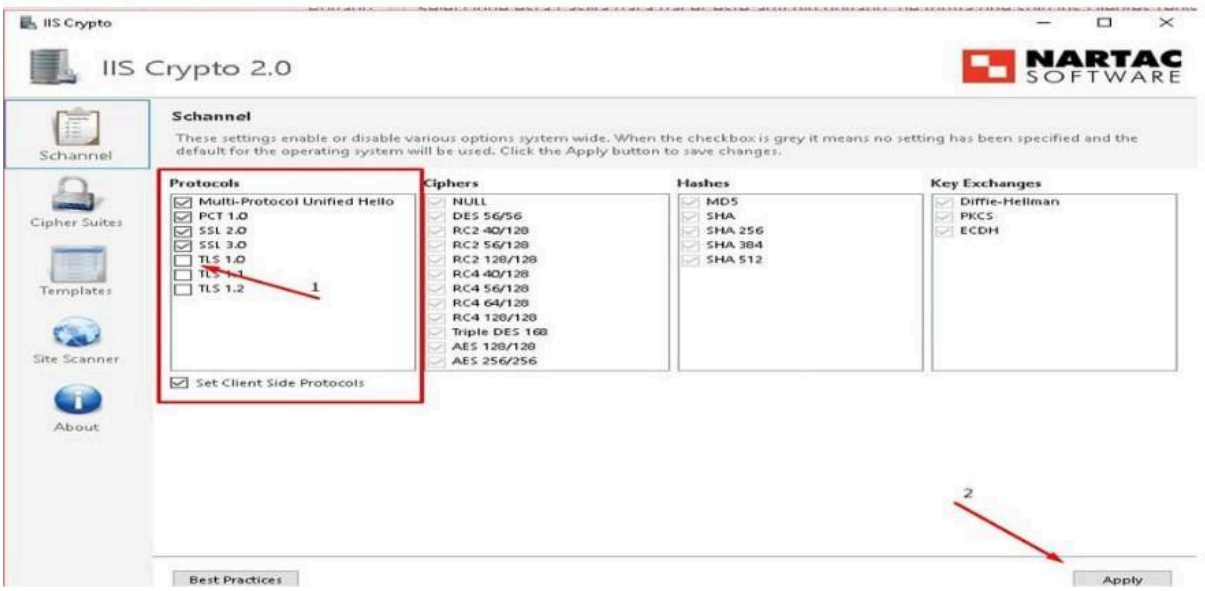
Actualización SSL/TLS
Fecha de Implementación: 07/04/24
Última Revisión: administradores de infraestructura
Versión: 1.0
I. Objetivo
Mejora de la Seguridad: Las versiones más recientes de SSL/TLS suelen abordar vulnerabilidades y debilidades encontradas en versiones anteriores. Al actualizar a versiones más nuevas, se implementan mejores prácticas de seguridad y se evitan posibles ataques, como BEAST, POODLE, Heartbleed, entre otros.
II. Alcance
el alcance de actualizar SSL/TLS abarca desde la actualización de servidores y clientes hasta la implementación de políticas de seguridad para garantizar conexiones seguras y protegidas en todos los sistemas y dispositivos involucrados en las comunicaciones en línea
III. Procedimiento para
actualizar 1 Descargar Nartac.
Lo primero sera iniciar el cliente de descargar para la herramienta Nartac la cual será la encargada de actualizar nuestros protocolos SSL y TLS a su ultima versión. Haga clic en el enlace a continuación (No tomará mas de dos minutos.).
https://www.nartac.com/Downloads/IISCrypto/IISCrypto.exe

2 Instalar Nartac
Luego de haberse completado la descarga haremos clic sobre el link de descarga para iniciar el proceso de instalación. Empezando por hacer clic en aceptar, lo cual indica que aceptamos los terminos y condiciones del servicio.



3 Configurar Nartac

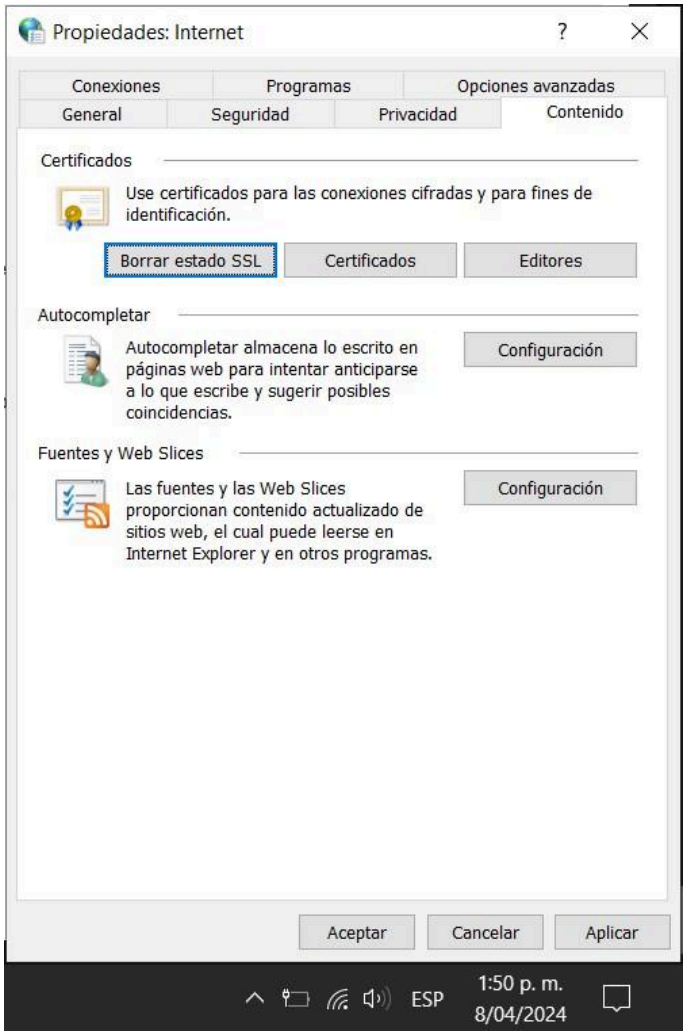
Luego de esto nos aparece una nueva pestaña donde seleccionaremos una a una, todas las opciones con respecto a actualizaciones para protocolos de seguridad, es decir SOLO la lista del menú «Protocols«. Como se muestra en la imagen a continuación.

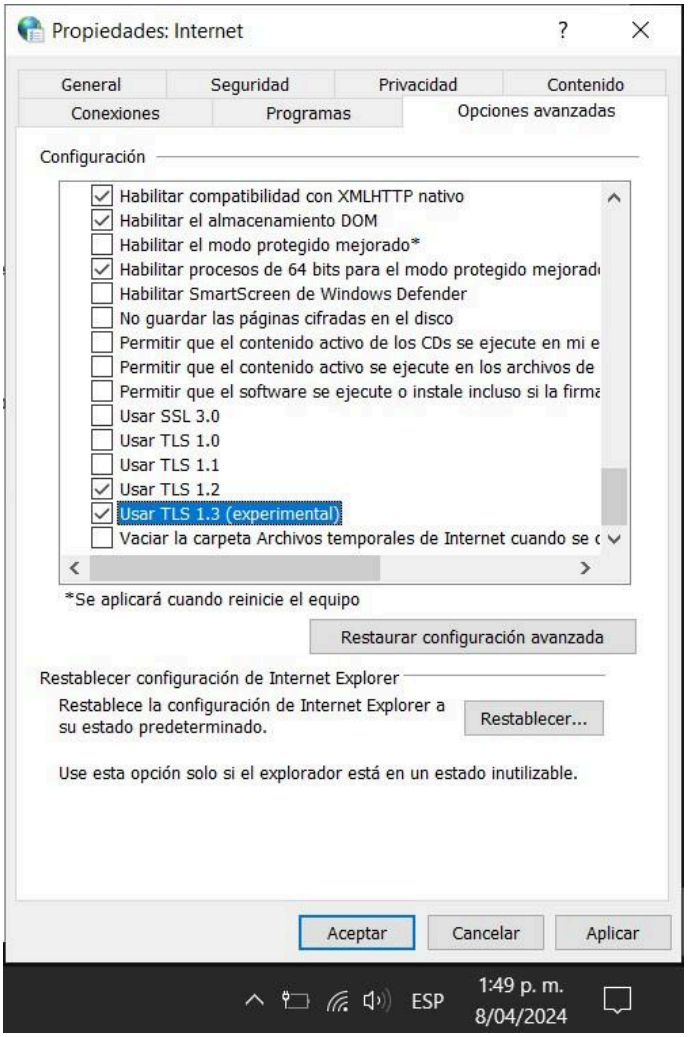


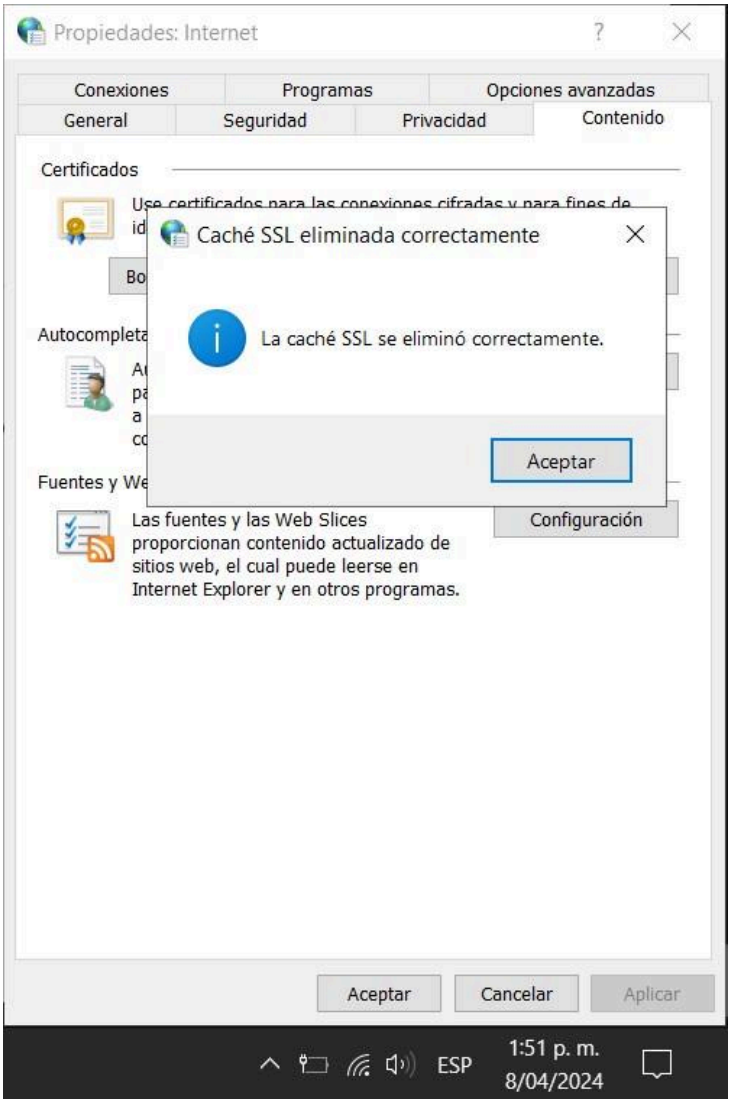

4 Aplicar cambios.
Una vez configurado haremos clic en aplicar o «Apply» e inmediatamente nos pedirá que reiniciemos el equipo para efectuar dichos cambios.

informacion tomada de
https://adclichosting.com/blog/actualizacion-de-protocolo-ssl-y-tls

Descripción de la vulnerabilidad:
Pasos de Reproducción

1. 

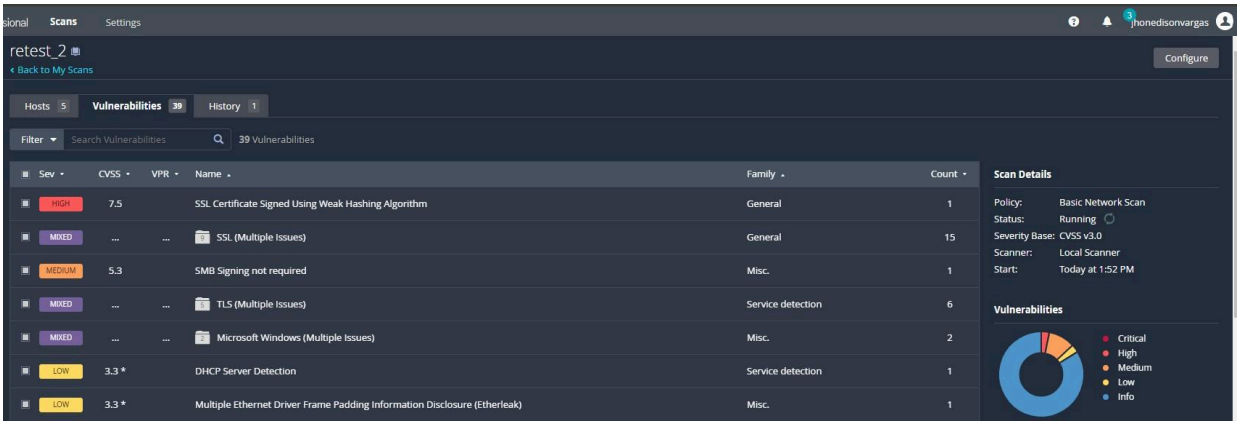
2. 
Propiedades: Internet
General
Seguridad
Privacidad
Contenido
Conexiones
Programas
Opciones avanzadas
Configuración
Habilitar compatibilidad con XMLHTTP nativo
Habilitar el almacenamiento DOM
Habilitar el modo protegido mejorado*
Habilitar procesos de 64 bits para el modo protegido mejorad
Habilitar SmartScreen de Windows Defender
No guardar las páginas cifradas en el disco
Permitir que el contenido activo de los CDs se ejecute en mi e
Permitir que el contenido activo se ejecute en los archivos de
Permitir que el software se ejecute o instale incluso si la firma
Usar SSL 3.0
Usar TLS 1.0
Usar TLS 1.1
Usar TLS 1.2
Usar TLS 1.3 (experimental)
Vaciar la carpeta Archivos temporales de Internet cuando se c
*Se aplicará cuando reinicie el equipo
Restaurar configuración avanzada
Restablecer configuración de Internet Explorer
Restablece la configuración de Internet Explorer a su estado predeterminado.
Restablecer...
Use esta opción solo si el explorador está en un estado inutilizable.
Aceptar
Cancelar
Aplicar
ESP
1:49 p. m.
8/04/2024

3. 


Solución de la Vulnerabilidad

Abrir el Panel de Control y dirigirse a "Configuración de Internet" u "Opciones de Internet".
En la pestaña "Avanzada", hacer clic en el botón "Configuración..." bajo "Seguridad".
En la lista de versiones de SSL y TLS, seleccionar las casillas para habilitar las últimas versiones de TLS (TLS 1.2 y TLS 1.3) y deshabilitar las versiones antiguas como SSL 2.0 y SSL 3.0.
Hacer clic en "Aceptar" para guardar los cambios.
Mantener actualizado Windows y los navegadores web instalados para asegurarse de tener los últimos parches de seguridad relacionados con SSL/TLS.
Resultado de la Solución
La implementación de la solución anterior ha mitigado la vulnerabilidad y mejorado la seguridad del sistema. Ahora se utilizan las versiones más recientes y seguras de SSL/TLS, lo que ayuda a proteger contra ataques que podrían explotar vulnerabilidades en las versiones más antiguas.

Retest de vulnerabilidad fue solucionada




Conclusión
La vulnerabilidad ha sido solventada satisfactoriamente siguiendo los pasos de la solución descrita. Se recomienda mantener un monitoreo constante y realizar actualizaciones periódicas para garantizar la seguridad continua del sistema.

Espero que esta plantilla te sea útil para crear tu informe de actualización de vulnerabilidad. Si tienes alguna pregunta adicional, no dudes en consultarme.

Equipo de Administración de Infraestructura