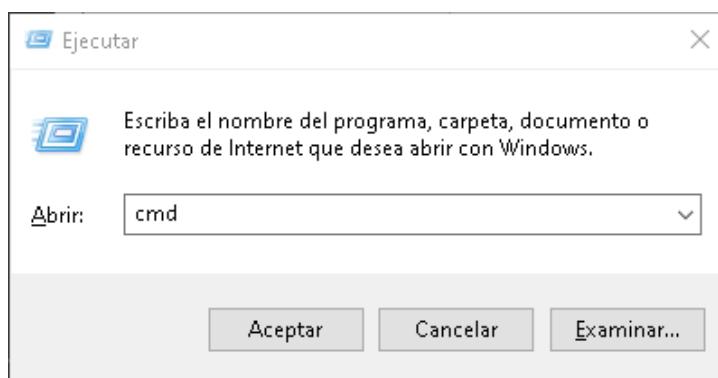


Cómo realizar actualizaciones en caso de encontrar vulnerabilidades en un endpoint de EMS:

Método n° 1: por CMD de manera manual.

(Tener en cuenta que debemos establecer la conexión mediante **anydesk** con el endpoint en el cual queremos realizar este proceso).

Abrimos la terminal (Tecla Windows+R) e ingresamos “cmd” y enter/aceptar.



Una vez en la terminal, ingresamos el comando “**winget upgrade**” el cual nos mostrará las actualizaciones disponibles del sistema.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 10.0.19045.4780]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Operador>winget upgrade
Nombre           Id          Versión      Disponible   Origen
-----
Mozilla Firefox (x64 en-US) Mozilla.Firefox    130.0.1     131        winget
Oracle VM VirtualBox 7.0.20 Oracle.VirtualBox 7.0.20     7.1.0      winget
Microsoft Edge      Microsoft.Edge    129.0.2792.65 129.0.2792.79 winget
WebView2 Runtime de Microsoft Edge Microsoft.EdgeWebView2Runtime 129.0.2792.65 129.0.2792.79 winget
4 actualizaciones disponibles.
```

Luego ingresamos el comando “**winget upgrade --all**” para actualizar todos los paquetes disponibles.

```
C:\Users\Operador>winget upgrade --all
```

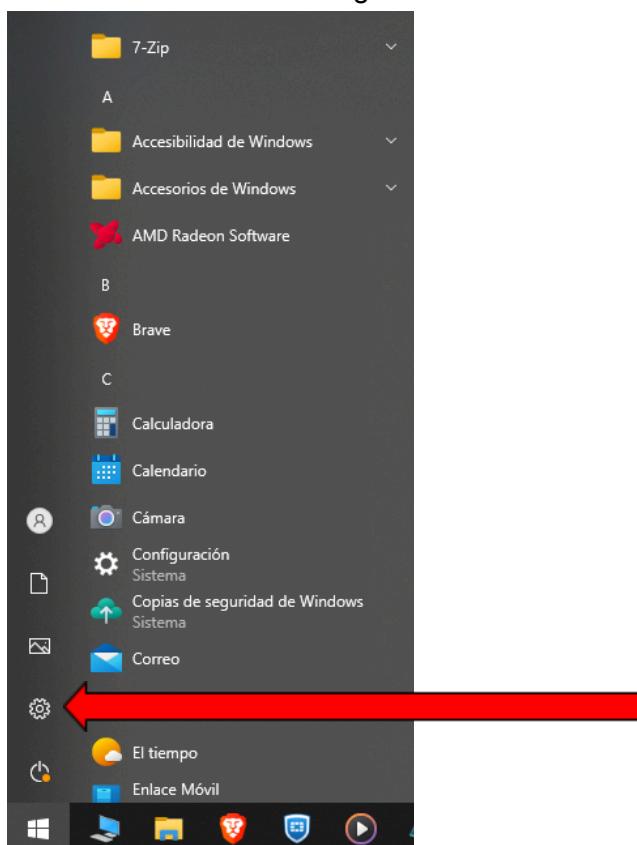
```
C:\Users\Operador>winget upgrade --all
Nombre           Id          Versión      Disponible   Origen
-----
Mozilla Firefox (x64 en-US) Mozilla.Firefox    130.0.1     131        winget
Oracle VM VirtualBox 7.0.20 Oracle.VirtualBox 7.0.20     7.1.0      winget
Microsoft Edge      Microsoft.Edge    129.0.2792.65 129.0.2792.79 winget
WebView2 Runtime de Microsoft Edge Microsoft.EdgeWebView2Runtime 129.0.2792.65 129.0.2792.79 winget
4 actualizaciones disponibles.

Instalando dependencias:
Este paquete requiere las siguientes dependencias:
- Paquetes
  Microsoft.VCRedist.2015+.x64
(1/3) Encontrado Mozilla Firefox [Mozilla.Firefox] Versión 131.0
El propietario de esta aplicación le concede una licencia.
Microsoft no es responsable, ni tampoco concede ninguna licencia de paquetes de terceros.
Descargando https://download-installer.cdn.mozilla.net/pub/firefox/releases/131.0/win64/es-MX/Firefox%20Setup%20131.0.exe
63.7 MB / 63.7 MB
```

Advertencia: El sistema va a pedir al usuario confirmar acción o pedir permiso para realizar acciones, por lo que se recomienda prestar atención a las ventanas emergentes que puedan surgir.

Por otro lado, tenemos que chequear las actualizaciones de Windows disponibles:

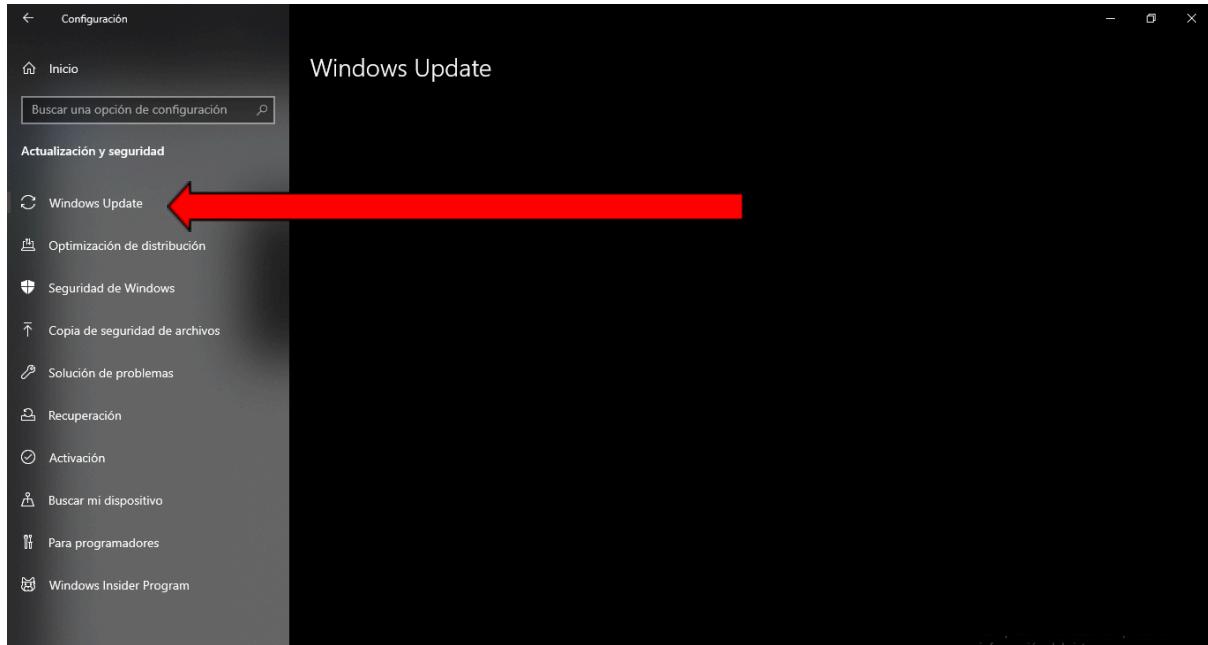
1. Presionar el símbolo del sistema, donde un menú va a desplegarse.
2. Hacer click en configuración.



Ir a “Actualización y Seguridad”

The image shows the Windows Settings interface in dark mode. At the top, there's a sign-in section for 'Operador' (Local account) with options to 'Iniciar sesión' or 'Omitir por ahora'. Below this is a search bar labeled 'Buscar una opción de configuración'. The main area contains several tiles: 'Sistema' (monitor icon), 'Dispositivos' (camera icon), 'Dispositivos móviles' (phone icon), 'Internet y red' (globe icon), 'Personalización' (paint palette icon), 'Aplicaciones' (grid icon), 'Cuentas' (person icon), 'Hora e idioma' (clock icon), 'Juegos' (game controller icon), 'Búsqueda' (magnifying glass icon), 'Privacidad' (padlock icon), and 'Accesibilidad' (handicap icon). A red box highlights the 'Actualización y seguridad' tile at the bottom center, which is described as 'Windows Update, recuperación, copia seg.'.

Entrar a “**Windows Update**” y verificar que el sistema no tenga ninguna actualización disponible, si la tiene se deberá actualizar de inmediato.



Método 2: Desde Forti Client.

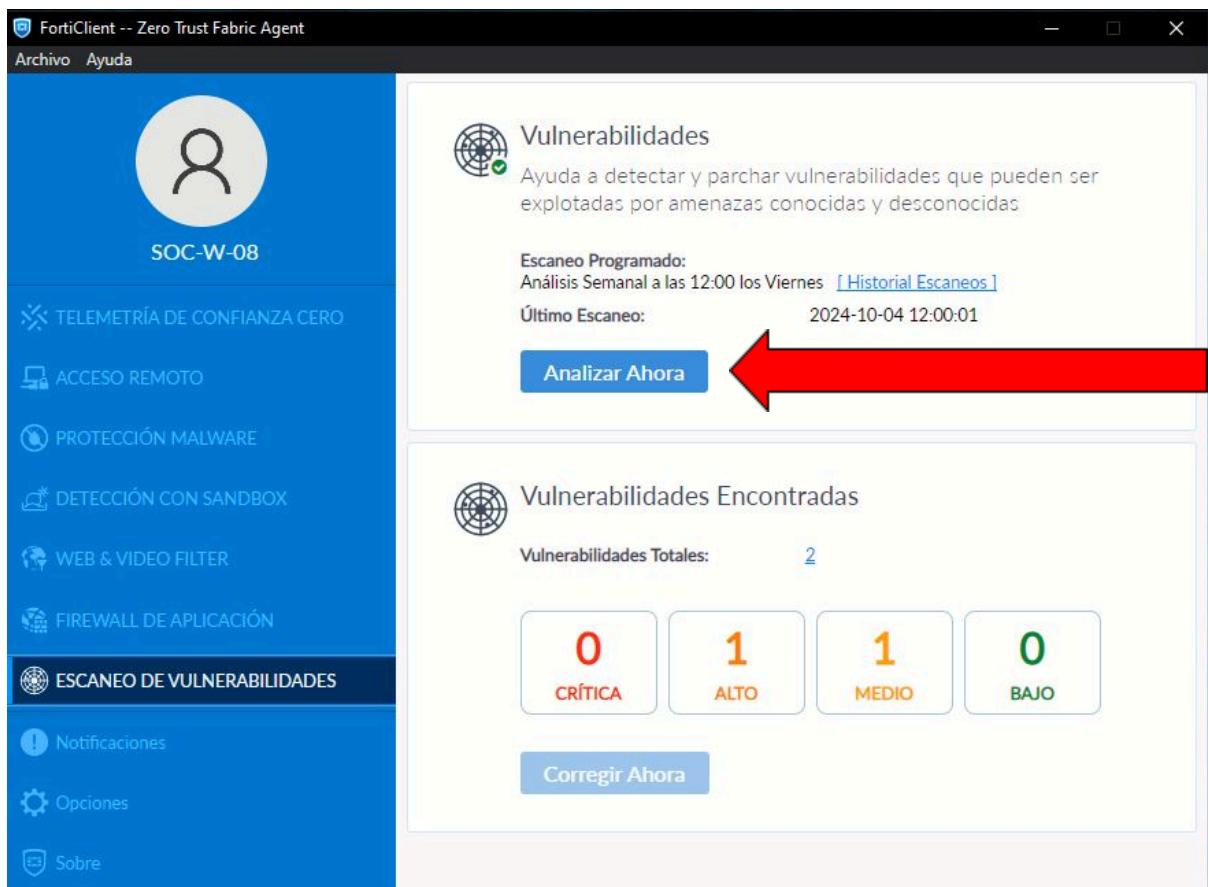
Abrir FortiClient.



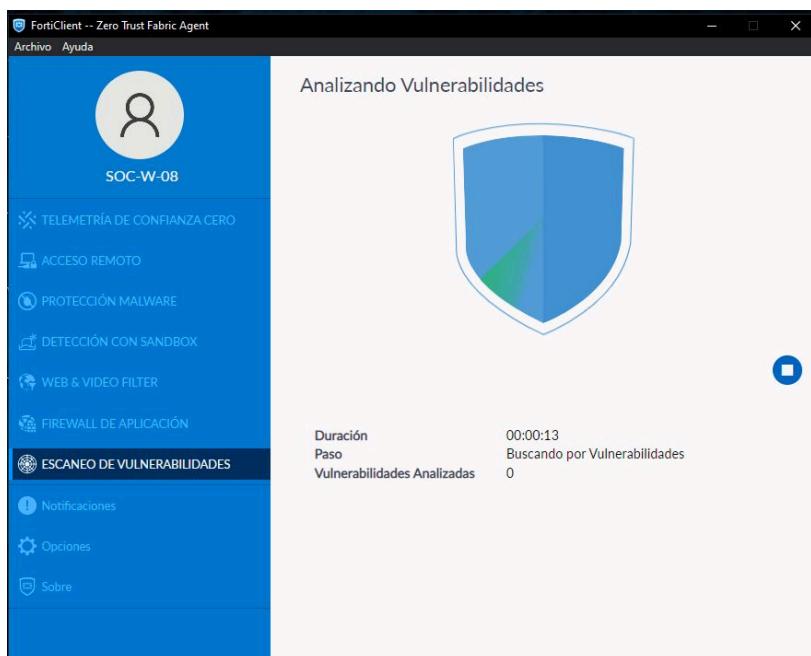
En la barra de menú del lado izquierdo, seleccionar la opción “**Escaneo de vulnerabilidades**”



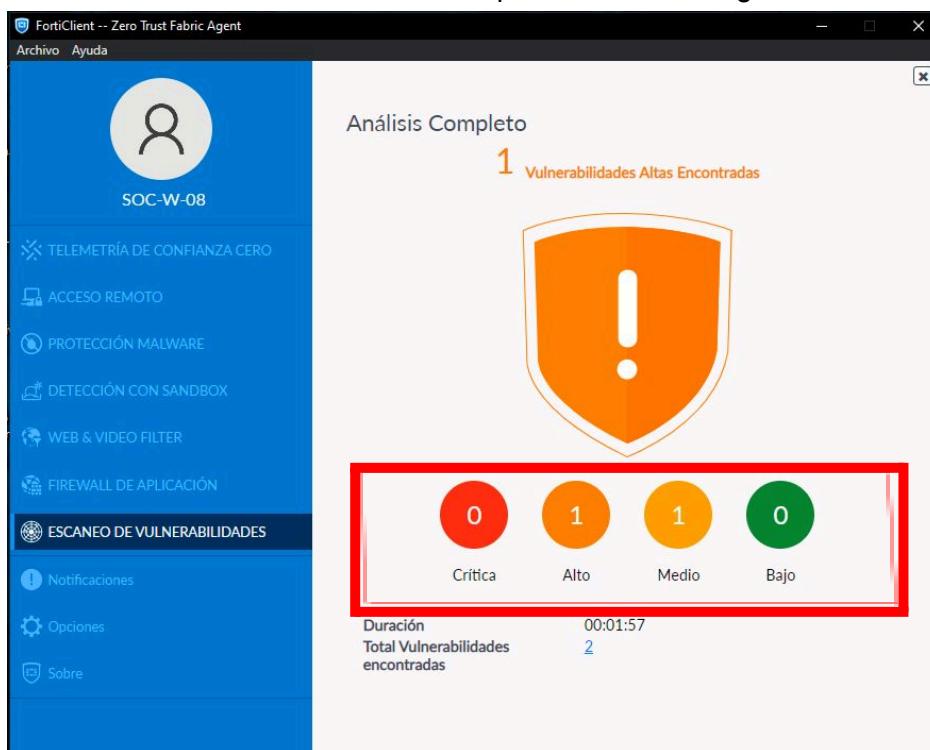
Una vez en la opción de “Escaneo de vulnerabilidades”, hacer click en el botón de “Analizar ahora”.



El sistema comenzará el escaneo de vulnerabilidades



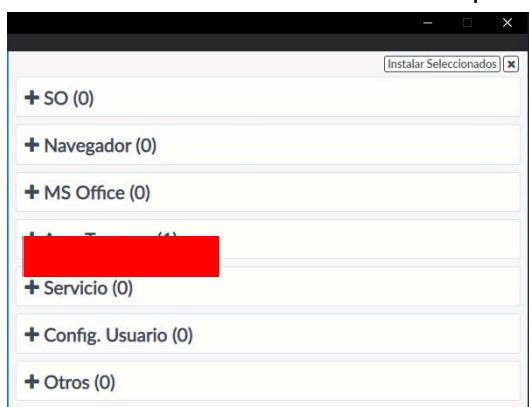
Cuando el análisis se complete vamos a poder ver en pantalla las **vulnerabilidades encontradas**, clasificadas en colores para identificar su gravedad.



Hacemos click en una de ellas



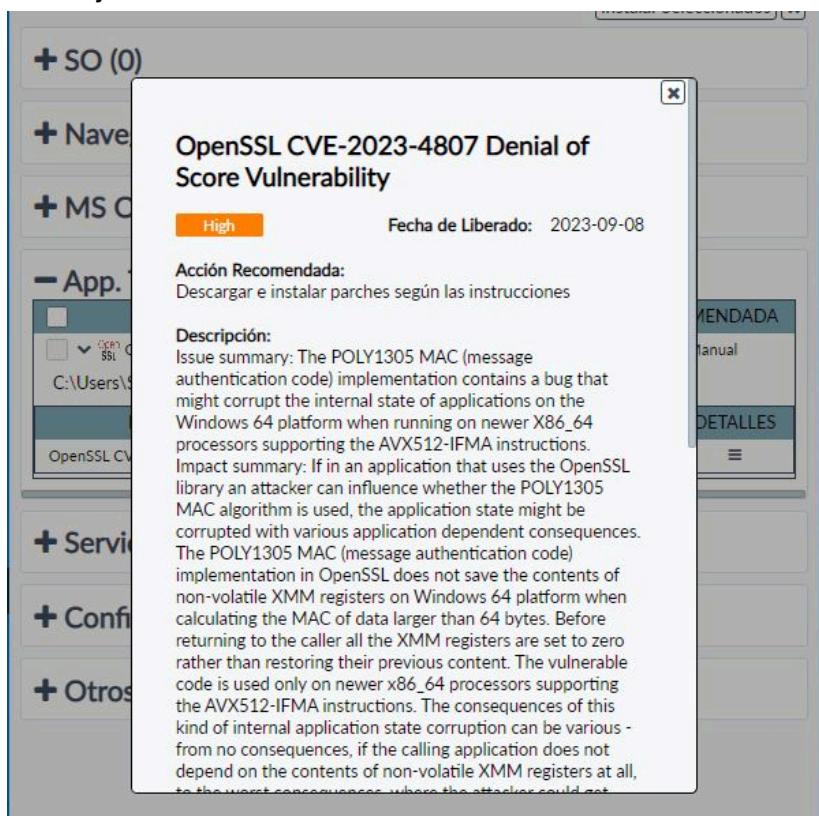
Al hacer click nos va a mostrar las opciones de vulnerabilidades que detectó.



Al hacer click en la vulnerabilidad (en este caso "App. Terceros") se despliega un renglón donde podemos visualizar el nombre de la vulnerabilidad, su severidad y una acción recomendada.

App. Terceros (1)		
APLICACIONES	SEVERIDAD	ACCIÓN RECOMENDADA
OpenSSL 1.1.1.22 (1)	High	Instalación Manual

Si hacemos click en la opción de la vulnerabilidad podemos visualizar información de la misma junto a su **CVE**.



Para culminar con la actualización, debemos seleccionar la opción de la vulnerabilidad marcando la casilla de la misma y presionando el botón de “**instalar seleccionados**” ubicado en el margen superior derecho.

