

viernes, 19 de julio de 2024

Guía para la solución de problema de arranque causado por update corrupto de CrowdStrike.

El 19 de julio de 2024, CrowdStrike sufrió una interrupción significativa que afectó a empresas en todo el mundo. Este problema comprometió la capacidad de las organizaciones para monitorear y responder a amenazas de ciberseguridad en tiempo real, afectando componentes críticos como la ingestión de telemetría, alertas, APIs y sistemas de notificación.

Para solucionar temporalmente la avería, se ha creado una guía que incluye los siguientes pasos:

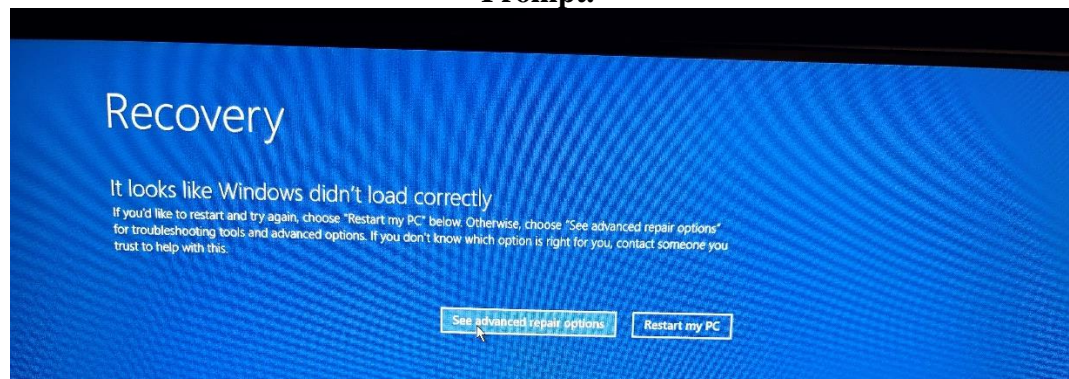
1. Arrancar Windows en Safe-Mode o en el Recovery mode de Windows.
2. Navegar a la carpeta de drivers de CrowdStrike.
3. Localizar y eliminar el archivo problemático identificado como “C-00000291*.sys”.
4. Reiniciar el equipo normalmente.

Además, se ha incluido una guía alternativa para realizar estos pasos usando el Command prompt (CMD) para aquellos usuarios que prefieran o necesiten esta opción. Esta guía asegura que los usuarios puedan eliminar el archivo problemático y reiniciar sus sistemas, ayudando a mitigar el impacto de la interrupción mientras CrowdStrike trabaja para restaurar completamente sus servicios.

Guía para Realizar los Pasos por CMD

Paso 1: Arrancar en Safe-Mode

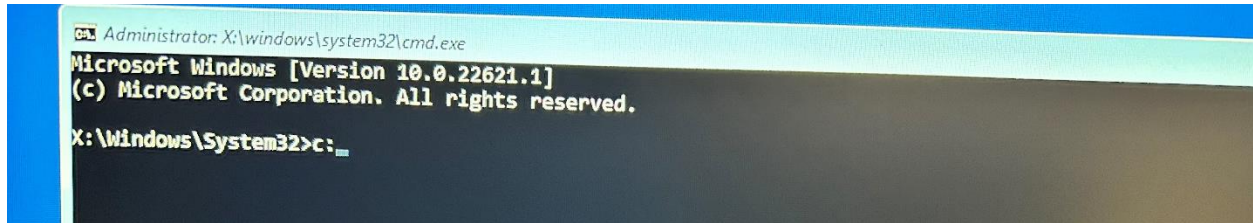
1. **Reiniciar el equipo:**
 - Reinicia el equipo.
 - Mientras el equipo está arrancando, presiona repetidamente la tecla **F8** hasta que aparezca el menú de opciones avanzadas de arranque.
2. **Seleccionar Safe-Mode:**
 - En el menú de opciones avanzadas, selecciona **Modo Seguro con Command Prompt**.



Paso 2: Navegar a la Carpeta de Drivers de CrowdStrike

1. Abrir CMD como Administrador:

- Una vez en Safe-Mode, se abrirá automáticamente la ventana de CMD.

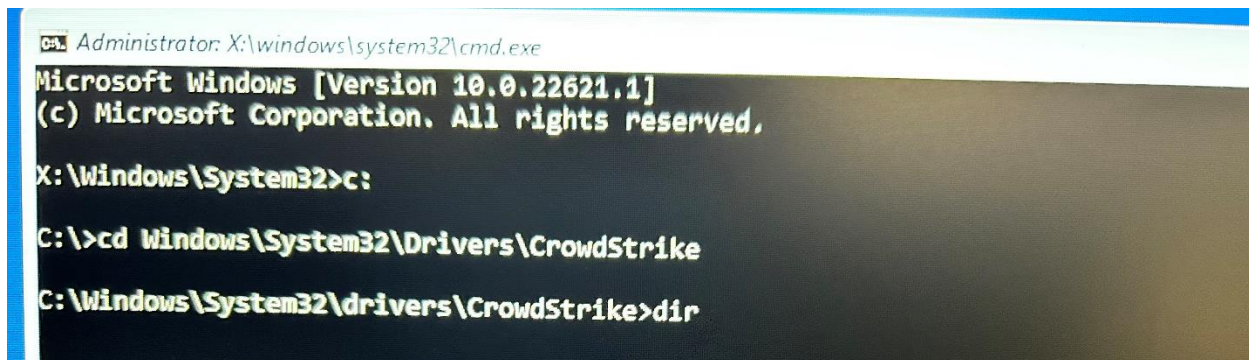


```
Administrator: X:\windows\system32\cmd.exe
Microsoft Windows [Version 10.0.22621.1]
(c) Microsoft Corporation. All rights reserved.

X:\Windows\System32>c: _
```

Navegar a la Carpeta Específica:

- En la ventana de CMD, escribe el siguiente comando y presiona **Enter**:
- C: enter
- Cd Windows\System32\drivers\CrowdStrike



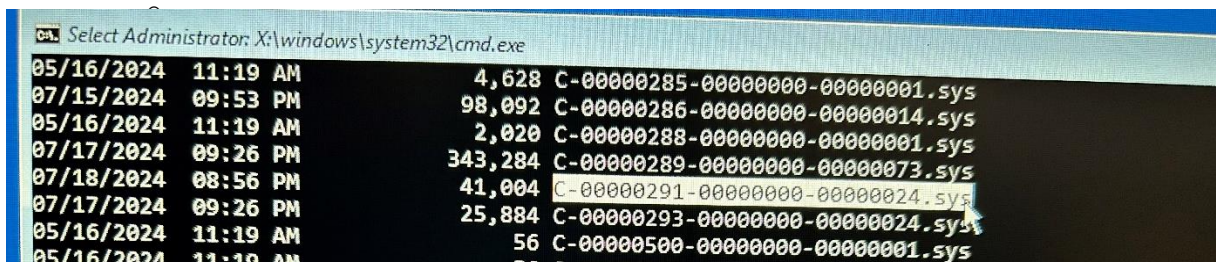
```
Administrator: X:\windows\system32\cmd.exe
Microsoft Windows [Version 10.0.22621.1]
(c) Microsoft Corporation. All rights reserved.

X:\Windows\System32>c:
C:\>cd Windows\System32\Drivers\CrowdStrike
C:\Windows\System32\drivers\CrowdStrike>dir
```

Paso 3: Localizar y Eliminar el Archivo

1. Buscar el Archivo:

- En la ventana de CMD, escribe el siguiente comando para listar los archivos que coinciden con el patrón:
- dir C-00000291*.sys ++(con fecha del 07/18/24)
- Localiza el archivo en la lista que aparece



```
Select Administrator: X:\windows\system32\cmd.exe
05/16/2024 11:19 AM          4,628 C-00000285-00000000-00000001.sys
07/15/2024 09:53 PM        98,092 C-00000286-00000000-00000014.sys
05/16/2024 11:19 AM          2,020 C-00000288-00000000-00000001.sys
07/17/2024 09:26 PM       343,284 C-00000289-00000000-00000073.sys
07/18/2024 08:56 PM        41,004 C-00000291-00000000-00000024.sys
07/17/2024 09:26 PM        25,884 C-00000293-00000000-00000024.sys
05/16/2024 11:19 AM           56 C-00000500-00000000-00000001.sys
05/16/2024 11:19 AM           55 C-00000500-00000000-00000001.sys
```

2. Eliminar el Archivo:

- En la ventana de CMD, escribe el siguiente comando y presiona **Enter**:
- del C-00000291*.sys

- Puedes copiar el nombre del archivo sombreado el archivo y presionando enter.

```
Administrator: X:\windows\system32\cmd.exe
06/03/2024 02:33 PM          1,174 f9af419786791f3c1dd8247b0655c2a72abcf720f9
07/09/2024 10:50 AM          134,112 Osfm-00000001.bin
06/21/2024 09:55 AM          134,648 Osfm-00000428.bin
06/26/2024 10:28 AM          134,632 Osfm-00000429.bin
07/10/2024 08:42 AM          134,632 Osfm-00000430.bin
07/16/2024 02:53 PM    <DIR>          Packages
07/17/2024 11:26 AM          2,967,913 SpotlightVCI-00000043.bin
06/03/2024 02:39 PM          33,554,456 UefiFirmwareImage.bin
          196 File(s)    158,952,110 bytes
           5 Dir(s)    411,954,311,168 bytes free

C:\Windows\System32\drivers\CrowdStrike>del C-00000291-00000000-00000024.sys
```

Paso 4: Reiniciar el Equipo

1. Reiniciar desde CMD:

- En la ventana de CMD, escribe el siguiente comando y presiona **Enter**:

```
shutdown /r
```

preparado por:

Poincaré Díaz Peña
Principal Oficial de Ciberseguridad
De Puerto Rico