Nro. Alerta:	EC-2024-15	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	TLP:BLANCO	**ALERTAS DE SEGURIDAD**	ecucert
Fecha:	22-jul-2024	**Crowdstrike - Windows**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Información.

Tipo de incidente: Información.

Nivel de riesgo: Medio

II. INTRODUCCIÓN

A raíz de la última actualización de CrowdStrike Falcon Sensor, se ha producido a nivel global un fallo que estaría generando errores en sistemas provistos por Microsoft Azure, Windows versiones 10 y 11, afectando al correcto funcionamiento de multitud de organizaciones. Cabe indicar que, en el momento de redacción de esta nota informativa, desde CrowdStrike informa que el fallo se ha corregido y que se encuentran trabajando en una solución oficial, aunque ya han surgido medidas paliativas para corregir el error ocasionado.

III. VECTOR DE ATAQUE:

El día 19 de julio de 2024, se han publicado información señalando que se ha producido un error a nivel global en los equipos que usan el software de seguridad de CrowdStrike Falcon Sensor bajo sistemas operativos Windows 10 y Windows 11. En concreto, numerosas organizaciones estarían experimentando errores conocidos como Blue Screen of Death (BSOD) alertando con el siguiente mensaje de error "DRIVER_OVERRAN_STACK_BUFFER", el que impide el arranque y correcto funcionamiento del sistema debido a la generación en bucle de este problema.

IV. INDICADORES DE COMPROMISO:

La función principal de CrowdStrike es la de detectar y prevenir posibles ciberataques, para evitar daños críticos a las empresas con las que trabaja. Una de estas, es precisamente Microsoft quien ha confirmado que la incidencia con sus plataformas es debido a un problema con CrowdStrike.

Dirección: Av. 9 de Octubre N27-75 y Berlín
Código postal: 170513 / Quito - Ecuador
Teléfono: +593-2 2946 400
www.arcotel.gob.ec

Nro. Alerta:	EC-2024-15	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	TLP:BLANCO	**ALERTAS DE SEGURIDAD**	ecucert
Fecha:	22-jul-2024	**Crowdstrike - Windows**	V 1.1

La incidencia de CrowdStrike está relacionada con una de sus principales herramientas: CrowdStrike Falcon Cloud Security. Se trata de una solución para "detener las infracciones en la nube".

Falcon es uno de los sistemas de protección para Windows. En el momento en que Falcon falla, los sistemas con Azure y Windows no pueden asegurar la seguridad del sistema y por ello se paraliza el sistema para evitar posibles daños. Desde CrowdStrike enviaron una actualización de controladores de Falcon con problemas. Azure **no reconoció** esta actualización y ha provocado la aparición de pantallazos azul en millones de sistemas y empresas.

Los ciberatacantes han aprovechado este escenario de falla, generando dominios maliciosos para descarga, mismos que se listan a continuación:

Dominios Maliciosos Detectados:

- Crowdstrikebluescreen.com
- crowdstrike0day.com
- crowdstrike-bsod.com
- crowdstrikedoomsday.com
- crowdstrikefix.com
- crowdstrikedown.site
- crowdstriketoken.com
- crowdstrike-helpdesk.com
- crashstrike.com
- bsodsm8r.xamzgjedu.com
- crowdstrikebsodfix.blob.core.windows.net
- crowdstrikecommuication.app
- fix-crowdstrike-apocalypse.com
- supportportal-crowdstrike-com.translate.goog
- crowdstrike-cloudtrail-storage-bb-126d5e.s3.us-west-1.amazonaws.com
- crowdstrikeoutage.info
- clownstrike.co.uk
- whatiscrowdstrike.com
- clownstrike.co
- microsoftcrowdstrike.com
- crowdfalcon-immed-update.com
- crowdstuck.org
- failstrike.com

Nro. Alerta:	EC-2024-15	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	TLP:BLANCO	**ALERTAS DE SEGURIDAD**	ecucert
Fecha:	22-jul-2024	**Crowdstrike - Windows**	V 1.1

- winsstrike.com
- t.me/Crowdstriketoken
- crowdstrikebluescreen.com
- crowdstrike0day.com
- crowdstrike-bsod.com
- crowdstrikedoomsday.com
- crowdstrikefix.com
- crowdstrikedown.site
- crowdstriketoken.com
- fix-crowdstrike-bsod.com

Los equipos que tienen acceso a las plataformas Microsoft que cumplen con las siguientes condiciones no experimentan errores relacionados con Falcon:

- Los hosts de Windows que no se han visto afectados no requieren ninguna acción, ya que el archivo de canal problemático se ha revertido.
- Los hosts de Windows que se compran en línea después de las 0527 UTC tampoco se verán afectados.
- Este problema no afecta a los hosts basados en Mac o Linux.
- El archivo de canal "C-00000291*.sys" con marca de tiempo de 0527 UTC o posterior es la versión revertida (buena).
- El archivo de canal "C-00000291*.sys" con la marca de tiempo 0409 UTC es la versión problemática.

V. IMÁGENES DE LA CAMPAÑA

Dirección: Av. 9 de Octubre N27-75 y Berlín
Código postal: 170513 / Quito - Ecuador
Teléfono: +593-2 2946 400
www.arcotel.gob.ec

Nro. Alerta:	EC-2024-15	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	TLP:BLANCO	**ALERTAS DE SEGURIDAD**	ecucert
Fecha:	22-jul-2024	**Crowdstrike - Windows**	V 1.1

VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

1. Mantenerse al pendiente de la información provista por CrowdStrike Engineering quienes han identificado una implementación de contenido relacionada con este problema y ha revertido esos cambios.

2. Mantenerse al pendiente de la información provista por Microsoft para solventar el problema. Es importante que se sigan los pasos indicados desde el fabricante.

3. Desde los fabricantes se han emitido las siguientes recomendaciones:

   En caso de que los equipos (hosts) aún se bloquean y no pueden permanecer en línea para recibir los cambios en el archivo de canal, se pueden usar los siguientes pasos para solucionar este problema:

   a. Reinicie el host para darle la oportunidad de descargar el archivo de canal revertido. Si el host se bloquea de nuevo, entonces:

      - Arranque Windows en modo seguro o en el entorno de recuperación de Windows
      - Vaya al directorio %WINDIR%\System32\drivers\CrowdStrike
      - Localice el archivo que coincida con "C-00000291*.sys" y elimínelo.
      - Arranque el host normalmente.

   b. Pasos alternativos para la nube pública o un entorno similar, incluido el virtual:

      Opción 1:

      - Desconecte el volumen de disco del sistema operativo del servidor virtual afectado
      - Cree una instantánea o una copia de seguridad del volumen de disco antes de continuar como precaución contra cambios no deseados
      - Adjuntar/montar el volumen en un nuevo servidor virtual
      - Vaya al directorio %WINDIR%\\System32\drivers\CrowdStrike
      - Localice el archivo que coincida con "C-00000291*.sys" y elimínelo.
      - Desconectar el volumen del nuevo servidor virtual
      - Vuelva a conectar el volumen fijo al servidor virtual afectado

Dirección: Av. 9 de Octubre N27-75 y Berlin
Código postal: 170513 / Quito - Ecuador
Teléfono: +593-2 2946 400
www.arcotel.gob.ec

Nro. Alerta:	EC-2024-15	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	TLP:BLANCO	**ALERTAS DE SEGURIDAD**	ecucert
Fecha:	22-jul-2024	**Crowdstrike - Windows**	V 1.1

Opción 2:

- Revertir a una instantánea anterior a las 0409 UTC.

Pasos de solución alternativa para Azure a través de serie:

- Inicie sesión en la consola de Azure --> Vaya a Máquinas virtuales --> seleccione la máquina virtual.
- Arriba a la izquierda en la consola --> Haga clic en "Conectar" --> Haga clic en --> Conectar --> Haga clic en "Más formas de conectarse" --> Haga clic en "Consola serie".
- Una vez que se haya cargado SAC, escriba 'cmd' y presione enter.
- Escriba el comando 'cmd'.
- Escriba : ch -si 1.
- Presione cualquier tecla (barra espaciadora). Introduzca las credenciales de administrador. Escriba lo siguiente:
  - bcdedit /set {current} safeboot mínimo
  - bcdedit /set {current} red de arranque seguro
  - Reiniciar la máquina virtual

Opcional: ¿Cómo confirmar el estado de arranque? Comando de ejecución:

- wmic COMPUTERSYSTEM GET BootupState

VII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VIII. REFERENCIAS:

https://www.xataka.com/seguridad/que-hace-crowdstrike-plataforma-ciberseguridad-para-microsoft-que-ha-provocado-caida-a-nivel-mundial

https://www.infobae.com/tecno/2024/07/20/crowdstrike-la-empresa-que-paralizo-computadoras-en-todo-el-mundo-afectando-a-microsoft/

Nro. Alerta:	EC-2024-15	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	TLP:BLANCO	**ALERTAS DE SEGURIDAD**	ecucert
Fecha:	22-jul-2024	**Crowdstrike - Windows**	V 1.1

https://www.infobae.com/america/mundo/2024/07/20/el-mundo-se-recupera-del-mayor-apagon-informatico-de-la-historia-causado-por-un-error-de-actualizacion-de-crowdstrike/

https://ciberseguridadtic.es/reportajes/los-principales-detalles-del-incidente-de-crowdstrike-y-microsoft-202407226156.htm