PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Asociación de Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

168-2024-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aéreadel Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y lasempresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°168	Fecha: 19-07-2024 Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Lo que hay que saber sobre el Stalkerware		
Tipo de Ataque	Spyware	Abreviatura	Spyware
Medios de propagación	USB, Disco, Red, Correo, Navegacion de Internet		
Código de familia	C	Código de Sub familia	C04
Clasificación temática familia	Código Malicioso		

Descripción

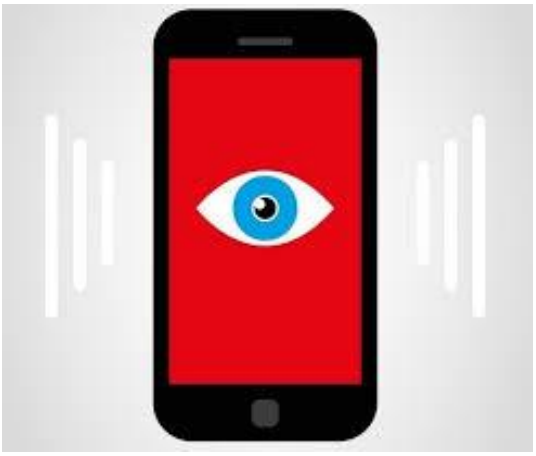
1. ANTECEDENTES:

El acoso digital tiene distintos tipos, y no tiene por qué asociarse a ciberdelincuentes o organizaciones criminales. En general, está relacionado con lo que son conocidas como relaciones tóxicas y que derivan al abuso y a la violencia de género. Es más, ya tiene un nombre: stalkerware.

2. DETALLES:

Stalkerware es un software comercial, por lo que no es necesario que se tengan grandes conocimientos informáticos para que el acosador lo utilice. De hecho, es un software que tiene una venta fácil y que se puede instalar por cualquiera. Solo es necesario el acceso físico al dispositivo móvil de la víctima.

En general, se descarga por alguien cercano, como un amigo íntimo, una pareja o incluso un familiar. La persona acosada en ningún momento sabe de la presencia de un stalkerware. Por lo tanto, no sabe que está bajo vigilancia de un acosador o acosadora. Lo delictivo reside en que grabar las acciones digitales de una persona es ilegal, ya que todo lo que la víctima vea en Internet se revela al acosador por medio del stalkerware. Y esto, aparte de violar el derecho a la privacidad y la intimidad digital, también puede conducir al chantaje, manipulación e incluso violencia física.



La persona que instala un stalkerware tiene información de absolutamente todo lo que contiene el dispositivo móvil de la víctima. Por ejemplo, conversaciones de WhastApp, llamadas telefónicas, emails, redes sociales, etc. Es decir, el control de la vida privada de una persona.

Para detectar este software de acoso, es común que el dispositivo móvil comience a funcionar lento, que use demasiado los datos móviles, que la cámara y el micrófono se activen solos y aleatoriamente, y que el dispositivo sufra sobrecalentamiento, o un rápido agotamiento de la batería.

3. RECOMENDACIONES:

- Restablecer los valores de fábrica, para eliminar el stalkerware. De esta manera se restablece la configuración original del dispositivo, por lo que deberás hacer una copia de seguridad de todo lo que no quieras perder.
- Habilitar la autenticación de dos factores cuando esté disponible para agregar una capa extra de seguridad a tus cuentas.
- Utilizar contraseñas únicas y robustas para cada sistema o aplicación, y realizar el cambio de contraseñas de forma periódica.
- Recomendar a los usuarios evitar acceder a información sensible, uso de servicios institucionales o realizar transacciones financieras a través de redes Wi-Fi abiertas.
- Verificar que el sistema operativo, aplicaciones y programas de antivirus estén actualizados para proteger contra vulnerabilidades conocidas y amenazas de seguridad.

Fuente de Información:	• hxxps://www.segurilatam.com/ciberilatam/el-stalkerware-la-nueva-forma-de-control-de-la-vida-privada-digital_20240717.html • hxxps://staysafeonline.org/es/resources/what-to-know-about-stalkerware/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°168	Fecha: 19-07-2024
		Página: 5 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica en Windows en Falcon Sensor CrowdStrike		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha detectado un problema de severidad **CRÍTICA** con el sensor Falcon de CrowdStrike que está afectando a varias estaciones de trabajo y servidores. Los síntomas incluyen reinicios inesperados, congelamientos y pantallas azules (BSOD).

2. DETALLES:

"CrowdStrike" es una herramienta de ciberseguridad utilizada por numerosas empresas para detener violaciones de seguridad y proteger contra amenazas digitales. El fallo reciente se identifica específicamente en la actualización del sensor Falcon de la compañía, que se instala en sistemas operativos Windows, Mac o Linux. La empresa emitió un mensaje grabado informando que estaban al tanto de los "informes de fallos en Windows relacionados con su sensor Falcon".

Microsoft y CrowdStrike trabajan conjuntamente para resolver esta incidencia que no ha sido categorizada como un ciberataque, sino como un defecto en una actualización de contenido para hosts de Windows.

El CEO de CrowdStrike, George Kurtz, confirmó que identificaron un "defecto" en una actualización de Windows, declarando que "esto no es un incidente de seguridad ni un ciberataque." Kurtz añadió que la actualización problemática ha sido aislada y se ha implementado una solución. También aseveró que la actualización solo afecta a dispositivos con Windows, no a Mac ni Linux.

CrowdStrike indicó que ha revertido los cambios que causaron estos fallos. Sin embargo, en algunos casos, los hosts afectados pueden no ser capaces de recibir estas actualizaciones automáticamente. En esos casos, será necesario realizar una intervención manual en modo de recuperación de Windows para solucionar el problema.

Cabe señalar que un **Workaround** es una solución temporal o una forma alternativa de resolver un problema o limitación en un sistema o software.

Workaround para los equipos que presentan los síntomas indicados:

- Iniciar Windows a modo prueba de fallos.
- Navegar al directorio **C:\Windows\System32\drivers\CrowdStrike**.
- Localizar el archivo **C-00000291*.sys** y borrarlo.
- Iniciar el equipo normalmente.

CrowdStrike agrega que para los equipos que utilizan **Bitlocker** para encriptar los hosts u otros sistemas similares a Bitlocker deberán contar con la llave de cifrado.

También en entornos en **Cloud** o similares deben realizarse los siguientes pasos para el workaround:

- Separar el volumen de disco del sistema operativo del servidor virtual afectado.
- Crear una instantánea o una copia de seguridad del volumen de disco antes de seguir adelante como medida de precaución contra cambios no deseados.
- Adjuntar/montar el volumen a un nuevo servidor virtual.

- Navegar al directorio C:\Windows\System32\drivers\CrowdStrike.
- Localizar el archivo **C-00000291*.sys** y borrarlos.
- Separar el volumen del nuevo servidor virtual.
- Volver a conectar el volumen fijo al servidor virtual afectado.

CrowdStrike informa que ha realizado las mitigaciones correspondientes. El archivo "**C-00000291*.sys**" con fecha de **0527 UTC** o posterior es la versión revertida la cual ya no genera problemas en los hosts. Por lo tanto, el archivo **C-00000291*.sys** con fecha y hora de **0409 UTC es la versión problemática** y que debería aplicarse sus respectivos **Workaround**.

Para los entornos Cloud o similares, incluye servidores virtuales, agregaron una segunda opción de workaround, se debe realizar el Roll back o revertir al snapshot antes de 0409 UTC.

Pasos de workaround para Azure vía Serial:

- Inicie sesión en la consola de Azure --> Vaya a Virtual Machines --> Seleccione la VM.
- Arriba a la izquierda en la consola --> Clic en: **Connect** --> Clic --> **Connect** --> Clic en **More ways to Connect** --> Clic en: **Serial Console**.
- Una vez cargado el SAC, teclea **'cmd'** y pulse **enter.**
  - Escriba el comando **cmd**.
  - Escriba: **ch -si 1**.
- Pulse cualquier tecla (barra espaciadora). Introduzca las credenciales de administrador;
- Escriba lo siguiente
  - **bcdedit /set {current} safeboot minimal**.
  - **bcdedit /set {current} safeboot network**.
- Reinicie la máquina virtual.

Opcional: ¿Cómo confirmar el estado de arranque? Ejecute el comando: **wmic COMPUTERSYSTEM GET BootupState.**

A. Productos afectados:

- Falcon Sensor CrowdStrike.

3. RECOMENDACIÓN:

- Realizar los pasos del workaround indicados por CrowdStrike.

Fuente de Información:	• hxxps://supportportal.crowdstrike.com/s/article/Tech-Alert-Windows-crashes-related-to-Falcon-Sensor-2024-07-19 • hxxps://azure.status.microsoft/en-gb/status

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°168	Fecha: 19-07-2024
		Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en la plataforma de gestión PowerSYSTEM Center de Subnet Solutions Inc.		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado una vulnerabilidad de severidad **MEDIA** de tipo contaminación prototipo que afecta a múltiples versiones de PowerSYSTEM Center de Subnet Solutions Inc. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto autenticado elevar los permisos dentro del sistema.

2. DETALLES:

PowerSYSTEM Center es una plataforma de gestión multifunción desarrollada por SUBNET Solutions, diseñada para la gestión de dispositivos electrónicos inteligentes (IED) de diversos fabricantes. Proporciona funcionalidades como la recopilación unificada de archivos de eventos, el almacenamiento y la gestión de IED, lo que la convierte en una herramienta vital para los sectores de servicios públicos e infraestructuras críticas.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2023-26136 de tipo contaminación prototipo que afecta a múltiples versiones de Subnet PowerSYSTEM Center, podrían permitir que un atacante autenticado eleve los permisos.

A. Productos afectados:

- PowerSYSTEM Center 2020: Update 20 y anteriores.

3. RECOMENDACIONES:

- Actualizar a la versión 2020 Update 21 o posterior de PowerSYSTEM Center para mitigar esta vulnerabilidad.
- Minimizar la exposición de la red para los dispositivos del sistema de control.
- Aislar las redes del sistema de control de las redes empresariales mediante firewalls.
- Utilizando métodos de acceso remoto seguros, como VPN.
- Realizar un análisis de impacto y evaluaciones de riesgos adecuados antes de implementar cualquier medida defensiva.

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-200-02

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°168	Fecha: 19-07-2024
		Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el enrutador inalámbrico Gigabit de banda dual DIR-823X AX3000 de D-Link v21_D240126		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo ejecución remota de código (RCE) con autorización en el enrutador inalámbrico Gigabit de banda dual DIR-823X AX3000 de D-Link v21_D240126. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante la ejecución remota de código en un dispositivo afectado. Un atacante que aproveche esta vulnerabilidad podría obtener acceso y control no autorizados del enrutador, lo que podría comprometer la seguridad de la red de los dispositivos conectados.

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-39962 de tipo ejecución remota de comandos en el enrutador inalámbrico Gigabit de banda dual DIR-823X AX3000 de D-Link v21_D240126, podría permitir a un atacante ejecutar código arbitrario en los enrutadores D-Link afectados de forma remota.

En esta versión de firmware, el servidor web no maneja correctamente el ntp_zone_valcampo en la solicitud CGI para /goform/set_ntp. Esto permite que un atacante cree un ntp_zone_valcampo malicioso y envíe una solicitud HTTP maliciosa a la /goform/set_ntpCGI, lo que lleva a la ejecución de comandos con privilegios de administrador en el sistema de archivos del firmware.

Una explotación exitosa podría llevar a la vulneración total del enrutador, lo que potencialmente permitiría a los atacantes interceptar o manipular el tráfico de red, usar el enrutador como punto de pivote para futuros ataques a la red o modificar la configuración del enrutador para su beneficio.

A. Productos afectados:

- Router inalámbrico Gigabit de banda dual DIR-823X AX3000 de D-Link v21_D240126.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de firmware disponible que aborda esta vulnerabilidad. Los usuarios deben consultar el sitio web de D-Link para obtener actualizaciones de seguridad o versiones de firmware que solucionen esta vulnerabilidad.
- Desactivar la administración remota del enrutador si no es necesaria.
- Implementar una segmentación de red sólida para aislar los enrutadores afectados.
- Monitorear los registros del enrutador para detectar cualquier actividad sospechosa.
- Considerar usar un firewall u otros dispositivos de seguridad de red para filtrar y monitorear el tráfico hacia y desde los enrutadores afectados.
- Considerar reemplazar el enrutador vulnerable con un modelo o marca diferente que no esté afectado por esta vulnerabilidad.

Fuente de Información:	• hxxps://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2024-39962 • hxxps://gist.github.com/Swind1er/40c33f1b1549028677cb4e2e5ef69109

Índice alfabético