Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

ACTUALIZACIÓN DEFECTUOSA DE CROWDSTRIKE PROVOCA CAÍDAS EN SISTEMAS WINDOWS

18/ 07 / 2024

CONTENIDO

INTRODUCCIÓN

Una actualización defectuosa lanzada por la empresa de ciberseguridad CrowdStrike ha provocado interrupciones masivas en estaciones de trabajo Windows a nivel mundial, afectando a una amplia gama de sectores desde instituciones financieras hasta aerolíneas. Aunque la compañía ha desplegado una solución y proporciona instrucciones para mitigar el problema, la recuperación completa podría tomar varios días, subrayando la fragilidad de las infraestructuras tecnológicas modernas y la necesidad de diversificación en los sistemas críticos.

ACTUALIZACIÓN DEFECTUOSA DE CROWDSTRIKE PROVOCA CAÍDAS EN SISTEMAS WINDOWS

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_07_19_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	19/07/2024
Es día cero (0 day):	No

RESUMEN

Empresas de todo el mundo han experimentado interrupciones generalizadas en sus estaciones de trabajo con Windows debido a una actualización defectuosa distribuida por la empresa de ciberseguridad CrowdStrike.

“En CrowdStrike estamos trabajando activamente con los clientes afectados por un defecto en una única actualización de contenido para hosts de Windows”, declaró George Kurtz, CEO de la compañía. “Los hosts de Mac y Linux no se han visto afectados. No se trata de un incidente de seguridad ni de un ciberataque”.

CROWDSTRIKE Platform Services Why CrowdStrike Learn Company

Statement on Falcon Content Update for Windows Hosts

CrowdStrike is actively working with customers impacted by a defect found in a single content update for Windows hosts. Mac and Linux hosts are not impacted. This is not a security incident or cyberattack.

The issue has been identified, isolated and a fix has been deployed. We refer customers to the support portal for the latest updates and will continue to provide complete and continuous updates on our website.

We further recommend organizations ensure they're communicating with CrowdStrike representatives through official channels.

Our team is fully mobilized to ensure the security and stability of CrowdStrike customers.

Actualización Defectuosa de CrowdStrike Provoca Caídas en Sistemas Windows, Impactando a Empresas a Nivel Mundial

La empresa en un comunicado dio a conocer “informes de pantallas azules de la muerte (BSOD) en hosts de Windows”, añadió que ha identificado el problema y ha desplegado una solución para su producto Falcon Sensor, instando a los clientes a consultar el portal de soporte para obtener las últimas actualizaciones.

Actualización Defectuosa de CrowdStrike Provoca Caídas en Sistemas Windows, Impactando a Empresas a Nivel MundialPara los sistemas que ya han sido afectados por el problema, las instrucciones de mitigación son las siguientes:

Iniciar Windows en Modo Seguro o en el Entorno de Recuperación de Windows.
Navegar al directorio C:\Windows\System32\drivers\CrowdStrike.
Encontrar el archivo nombrado “C-00000291*.sys” y eliminarlo.
Reiniciar el equipo o servidor normalmente.
Cabe destacar que la interrupción también ha afectado a Google Cloud Compute Engine, causando que las máquinas virtuales de Windows que usan el csagent.sys de CrowdStrike se bloqueen y entren en un estado de reinicio inesperado.

“Después de recibir automáticamente un parche defectuoso de CrowdStrike, las máquinas virtuales de Windows se bloquean y no pueden reiniciarse”, indicó Google Cloud. “Las máquinas virtuales de Windows que actualmente están en funcionamiento ya no deberían verse afectadas”.

Microsoft Azure también ha publicado una actualización similar, afirmando que “ha recibido informes de recuperación exitosa de algunos clientes que intentaron múltiples operaciones de reinicio de máquinas virtuales afectadas” y que “pueden ser necesarios varios reinicios (hasta 15)”.

Amazon Web Services (AWS), por su parte, dijo que ha tomado medidas para mitigar el problema en tantas instancias de Windows, Workspaces de Windows y Aplicaciones Appstream como sea posible, recomendando a los clientes aún afectados que “tomen medidas para restaurar la conectividad”.

El investigador de seguridad Kevin Beaumont comentó: “He obtenido el controlador de CrowdStrike que se distribuyó mediante la actualización automática. No sé cómo ocurrió, pero el archivo no es un controlador válidamente formateado y hace que Windows se bloquee cada vez”.

“CrowdStrike es el producto EDR de primera categoría, y está en todo, desde puntos de venta hasta cajeros automáticos, etc. – esto probablemente será el mayor incidente ‘cibernético’ en términos de impacto a nivel mundial.”

Aerolineas, instituciones financieras, cadenas de alimentación y retail, hospitales, hoteles, organizaciones de noticias, redes ferroviarias y empresas de telecomunicaciones se encuentran entre las muchas empresas afectadas. Las acciones de CrowdStrike han caído un 15% en el premercado estadounidense.

“Omer Grossman, Director de Información (CIO) de CyberArk, afirmó en una declaración compartida con los medios: “El evento actual parece – incluso en julio – ser uno de los problemas cibernéticos más significativos de 2024. El daño a los procesos empresariales a nivel global es dramático. El fallo se debe a una actualización de software del producto EDR de CrowdStrike.”

“Este es un producto que funciona con altos privilegios y protege los endpoints. Un mal funcionamiento en esto puede, como estamos viendo en el incidente actual, causar que el sistema operativo se bloquee.”

Se espera que la recuperación tome días, ya que el problema debe ser resuelto manualmente, endpoint por endpoint, iniciándolos en Modo Seguro y eliminando el controlador defectuoso, señaló Grossman, añadiendo que la causa raíz del mal funcionamiento será de “máximo interés”.

Jake Moore, asesor de seguridad global de la empresa eslovaca de ciberseguridad ESET, dijo que el incidente subraya la necesidad de implementar múltiples “seguros” y diversificar la infraestructura de TI.

“Las actualizaciones y el mantenimiento de sistemas y redes pueden incluir inadvertidamente pequeños errores, que pueden tener consecuencias de gran alcance como las experimentadas hoy por los clientes de CrowdStrike,” comentó Moore.

“Otro aspecto de este incidente se relaciona con la ‘diversidad’ en el uso de infraestructura de TI a gran escala. Esto se aplica a sistemas críticos como sistemas operativos, productos de ciberseguridad y otras aplicaciones desplegadas globalmente. Donde la diversidad es baja, un solo incidente técnico, por no mencionar un problema de seguridad, puede llevar a interrupciones a escala global con efectos posteriores.”

El desarrollo se produce mientras Microsoft se recupera de una interrupción separada que causó problemas con las aplicaciones y servicios de Microsoft 365, incluidos Defender, Intune, OneNote, OneDrive for Business, SharePoint Online, Windows 365, Viva Engage y Purview.

“Un cambio de configuración en una parte de nuestras cargas de trabajo de backend de Azure, causó una interrupción entre los recursos de almacenamiento y computo que resultó en fallos de conectividad que afectaron a los servicios de Microsoft 365 dependientes de estas conexiones,” dijo el gigante tecnológico.

Omkhar Arasaratnam, gerente general de OpenSSF, dijo que las interrupciones de Microsoft y CrowdStrike subrayan la fragilidad de las cadenas de suministro monoculturales y enfatizó la importancia de la diversidad en los stacks tecnológicos para una mayor resiliencia y seguridad.

“Las cadenas de suministro monoculturales (un solo sistema operativo, un solo EDR) son inherentemente frágiles y susceptibles a fallos sistémicos – como hemos visto,” señaló Arasaratnam. “La buena ingeniería de sistemas nos dice que los cambios en estos sistemas deben implementarse gradualmente, observando el impacto en pequeñas tranches en lugar de todos a la vez. Los ecosistemas más diversos pueden tolerar cambios rápidos ya que son resilientes a problemas sistémicos.”

NOTICIA COMPLETA

https://devel.group/blog/actualizacion-defectuosa-de-crowdstrike-provoca-caidas-en-sistemas-windows/

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente