CSIRT-DATASEC

DataSec

Boletín Ciberseguridad

TLP: CLEAR

26.06.2024

CLICK PARA EMPEZAR

En esta edición → Ataque Ransomware a hospitales de Londres

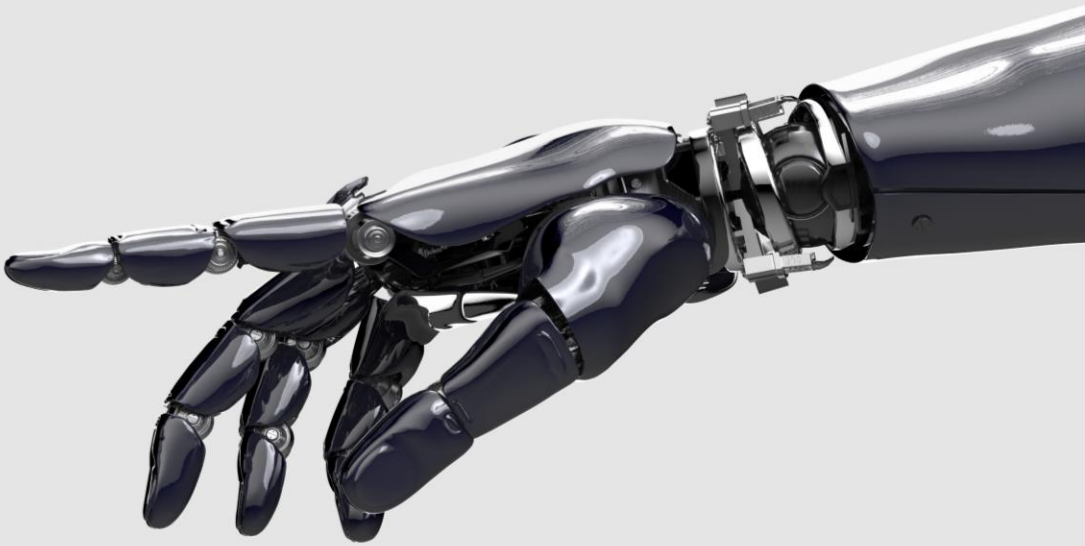
CONTENIDO

NUESTRA ESENCIA

VULNERABILIDADES

NOTICIAS

RECOMENDACIONES



Nos complace presentarles nuestro boletín de ciberseguridad, creado para mantener a nuestros lectores informados y seguros en un entorno digital en constante evolución. Ofrecemos una selección cuidadosa de contenido que cubre diversas temáticas, desde las últimas amenazas y vulnerabilidades hasta las mejores prácticas y soluciones de protección.

Datasec es una empresa colombiana líder en servicios tecnológicos, enfocada en la implementación, administración, soporte, monitoreo y gestión de plataformas de Seguridad Informática y Networking. Con una amplia experiencia en proyectos de ciberseguridad y conectividad para diversos sectores, tanto públicos como privados. Nuestro Centro de Operaciones de Seguridad Cibernética (CSOC) centraliza la detección, análisis y respuesta a amenazas, contribuyendo a la prevención y mitigación de incidentes en tiempo real.

IBM i privilege escalation

CVE-2024-27275

(7.4)

Impacto: Escalada de privilegios.

Resumen: IBM i 7.2, 7.3, 7.4 y 7.5 contiene una vulnerabilidad de escalada de privilegios local causada por un requisito de autoridad insuficiente. Un usuario local sin privilegio de administrador puede configurar un disparador de archivo físico para ejecutar con los privilegios de un usuario socialmente diseñado para acceder al archivo de destino. La corrección es exigir el privilegio del administrador para configurar el soporte desencadenante.

Versiones Afectadas

- BM i 7.5
- IBM i 7.4
- IBM i 7.3
- IBM i 7.2

Solución: Se recomienda aplicar las actualizaciones sugeridas en: https://www.ibm.com/support/pages/node/7157637?_ga=2.230003545.431680978.1718977080-461761459.1716304005

Fecha de Publicación: 14/JUN/2024

INFO

Cisco Secure Email and Web Manager and Secure Email Gateway Reflected Cross-Site Scripting Vulnerability

CVE-2024-20258

(6.1)

Impacto: Ejecución de código o comandos no autorizados.

Resumen: Un atacante podría explotar esta vulnerabilidad persuadiendo a un usuario de una interfaz afectada para hacer clic en un enlace manipulado. Un exploit exitoso podría permitir al atacante ejecutar código de script arbitrario en el contexto de la interfaz afectada o acceder a información sensible basada en el navegador.

Versiones Afectadas

- Cisco Secure Email and Web Manager versión 15.5 y anteriores.
- Secure Email Gateway versión 15.5 y anteriores.
- Secure Web Appliance versión 15.0 y anteriores.

Solución: Cisco ha lanzado actualizaciones de software que abordan esta vulnerabilidad. Consulte en + INFO.

Fecha de Publicación: 12/JUN/2024

INFO

IBM i privilege escalation

CVE-2024-31890

(7.8)

Impacto: Escalada de privilegios.

Resumen: El producto IBM TCP/IP Connectivity Utilities para i de IBM i 7.3, 7.4 y 7.5 contiene una vulnerabilidad local de elevación de privilegios. Un actor malicioso con acceso a la línea de comandos del sistema operativo host puede elevar sus privilegios y obtener acceso root al sistema.

Versiones Afectadas

- IBM i 7.5
- IBM i 7.4
- IBM i 7.3

Solución: Se recomienda aplicar las actualizaciones sugeridas en: https://www.ibm.com/support/pages/node/7158240?_ga=2.254414536.194951536.1719248224-461761459.1716304005

Fecha de Publicación: 20/JUN/2024

INFO

IBM Security SOAR code execution

CVE-2024-38319

(7.5)

Impacto: Ejecución de código o comandos no autorizados.

Resumen: IBM Security SOAR 51.0.2.0 podría permitir a un usuario autenticado ejecutar código malicioso cargado desde un script especialmente diseñado.

Versiones Afectadas

- IBM Security SOAR 51.0.2.0 and earlier

Solución: Se recomienda aplicar las actualizaciones sugeridas en: https://www.ibm.com/support/pages/node/7158261?_ga=2.48392038.194951536.1719248224-461761459.1716304005

Fecha de Publicación: 21/JUN/2024

INFO

IBM Storage Protect for Virtual Environments: Data Protection for VMware security bypass

CVE-2024-38329

(7.7)

Impacto: Escalada de privilegios.

Resumen: IBM Storage Protect para entornos virtuales: Data Protection for VMware 8.1.0.0 a 8.1.22.0 podría permitir a un atacante remoto autenticado saltarse las restricciones de seguridad, debido a una validación incorrecta de los permisos de usuario.

Versiones Afectadas

- IBM Storage Protect for Virtual Environments: Data Protection for VMware 8.1.0.0 - 8.1.22.0

Solución: Se recomienda aplicar las actualizaciones sugeridas en: https://www.ibm.com/support/pages/node/7157929?_ga=2.55077739.194951536.1719248224-461761459.1716304005

Fecha de Publicación: 18/JUN/2024

INFO

IBM WebSphere Application Server identity spoofing

CVE-2024-37532

(8.8)

Impacto: Escalada de privilegios.

Resumen: IBM WebSphere Application Server 8.5 y 9.0 es vulnerable a la suplantación de identidad por parte de un usuario autenticado debido a una validación de firma incorrecta.

Versiones Afectadas

- IBM WebSphere Application Server 9.0
- IBM WebSphere Application Server 8.5

Solución: Se recomienda aplicar las actualizaciones sugeridas en: https://www.ibm.com/support/pages/node/7158031?_ga=2.157443066.194951536.1719248224-461761459.1716304005

Fecha de Publicación: 19/JUN/2024

INFO

Adobe – Actualización de productos

CVE-2024-30299, CVE-2024-34102, CVE-2024-30300, CVE-2024-34108.

Adobe ha lanzado actualizaciones. Estas actualizaciones resuelven vulnerabilidades críticas, importantes y moderadas. La explotación exitosa de estas vulnerabilidades podría dar lugar a la ejecución arbitraria de código, lectura arbitraria de sistemas de archivos y derivación de la función de seguridad.

Recomendación: Se recomienda actualizar a la última versión disponible de los productos afectados siguiendo las instrucciones de seguridad disponibles en la página oficial.

Versiones Afectadas

- Adobe ColdFusion
- Adobe Commerce
- Adobe Creative Cloud Desktop Application
- Adobe Experience Manager
- Adobe FrameMaker Publishing Server
- Adobe Photoshop
- Adobe Substance 3D Stager

Fecha de Publicación: 19/JUN/2024

INFO

Google Chrome – Actualización de productos

CVE-2024-5274

Google ha emitido una actualización de seguridad de Chrome 126, abordando seis vulnerabilidades, incluyendo un defecto, rastreado como CVE-2024-6100 que se demostró durante el SSD Secure Disclosure-s TyphoonPWN 2024. TyphoonPWN es una competición de hackeo en vivo que se celebra anualmente en TyphoonCon, una conferencia de seguridad ofensiva en Seúl, Corea del Sur.

Recomendación: Se recomienda actualizar Google Chrome a la última versión disponible para Windows, MacOS y Linux desde la página oficial.

Versiones Afectadas

- Versiones anteriores a 126.0.6478.56 /57 para Windows y macOS.
- Versiones anteriores a 126.0.6478.54 para Linux.

INFO

Vmware – Actualización de productos

CVE-2024-37079, CVE-2024-37080, CVE-2024-37081

Varias vulnerabilidades de desbordamiento de heap y escalada de privilegios en vCenter Server se notificaron responsablemente a VMware. Hay actualizaciones disponibles para corregir estas vulnerabilidades en los productos de VMware afectados.
Un actor malicioso con acceso de red a vCenter Server puede desencadenar estas vulnerabilidades mediante el envío de un paquete de red especialmente diseñado que puede conducir a la ejecución remota de código.

Recomendación: Actualizar el producto afectado a la versión más reciente desde la página oficial del fabricante.

Versiones Afectadas

- VMware vCenter Server
- VMware Cloud Foundation

Fecha de Publicación: 18/JUN/2024

INFO

Microsoft – Actualización de productos

CVE-2024-30080, CVE-2024-30064, CVE-2024-30078, CVE-2024-30068, CVE-2024-30097, CVE-2024-30103,

Microsoft ha lanzado actualizaciones de seguridad que resuelven un total de 49 nuevas vulnerabilidades, incluidas, según su gravedad, 1 crítica, 36 altas y 12 medias.

Recomendación: Se recomienda a los usuarios y administradores revisar lo siguiente y aplicar las actualizaciones necesarias: Ver +INFO.

Aplicable para :

- Máquinas virtuales de ciencia de datos de Azure.
- Sincronización de archivos de Azure.
- monitor azul.
- SDK de Azure.
- Biblioteca de almacenamiento de Azure.
- Dinámica Central de Negocios.
- Entre otros.

Fecha de Publicación: 17/JUN/2024

INFO

LE PUEDE INTERESAR

Fecha de Publicación	Fabricante	CVE / Acceso	CVSSv3	Descripción
14/06/2024	Cisco	CVE-2024-20257 CVE-2024-20383 CVE-2024-20256	4.8	Una vulnerabilidad en la interfaz de gestión basada en web de Cisco AsyncOS Software para Cisco Secure Email Gateway podría permitir a un atacante remoto autenticado realizar un ataque XSS contra un usuario de la interfaz.
18/06/2024	VMware	CVE-2024-37079 CVE-2024-37080 CVE-2024-37081	9.8	VMware abordó múltiples vulnerabilidades vCenter Server que los atacantes remotos pueden explotar para lograr la ejecución remota de código o la escalada de privilegios. vCenter Server es una plataforma de gestión centralizada desarrollada por VMware para la gestión de entornos virtualizados.
14/06/2024	IBM	CVE-2024-31870	3.3	Esto puede ser utilizado por un actor malicioso para recopilar información sobre los usuarios que puede ser objetivo de otros ataques.
17/06/2024	IBM	CVE-2023-47726	7.1	Podrían permitir a un usuario autenticado ejecutar determinados comandos arbitrarios debido a una validación de entrada incorrecta.
25/06/2024	Linux	CVE-2024-39371	N/A	En el kernel de Linux, se ha resuelto la siguiente vulnerabilidad: io_uring: check for non-NULL file pointer in io_file_can_poll() En kernels anteriores, era posible desencadenar una desreferencia de puntero NULL fuera de la ruta de preparación asíncrona forzada, si no se había asignado ningún archivo.
25/06/2024	Linux	CVE-2024-39470	N/A	En el kernel de Linux, se ha resuelto la siguiente vulnerabilidad: eventfs: Fix a possible null pointer dereference in eventfs_find_events() En la función eventfs_find_events,hay un posible puntero nulo que puede ser causado por llamar a update_events_attr que realizará algunas operaciones en los miembros de la estructura ei cuando ei es NULL.
26/06/2024	WordPress	CVE-2024-5215	6.4	El plugin HT Mega - Absolute Addons For Elementor para WordPress es vulnerable a Stored Cross-Site Scripting a través de múltiples widgets en todas las versiones hasta, e incluyendo, 2.5.5 debido a insuficiente sanitización de entrada y escape de salida en atributos suministrados por el usuario.

Outlook desactiva la autenticación básica (nombre de usuario y contraseña)

Microsoft está implementando cambios significativos en sus métodos de autenticación para mejorar la seguridad de los usuarios de Outlook. La autenticación básica, que envía credenciales sin cifrar y las almacena en caché, está siendo reemplazada por autenticación basada en tokens y respaldada por autenticación multifactor (MFA). Esto significa que después del 16 de septiembre, las aplicaciones que solo admiten autenticación básica ya no podrán acceder a las cuentas de Outlook.com, Hotmail.com o Live.com. Los usuarios deberán cambiar a versiones más recientes de clientes de correo electrónico que soporten autenticación moderna, como las últimas versiones de Outlook, Apple Mail y Thunderbird.

Además, Microsoft anunció la desactivación de las aplicaciones Mail y Calendar, que estarán disponibles en Microsoft Store hasta el 31 de diciembre de 2024. Se anima a los usuarios a migrar al nuevo Outlook para Windows, que ofrece mayor seguridad.

Fecha de Publicación: 17/JUN/2024

Resumen

Microsoft ha anunciado nuevas mejoras de ciberseguridad para las cuentas de correo electrónico personales de Outlook como parte de su 'Iniciativa Futuro Seguro', incluida la desactivación de la autenticación básica (nombre de usuario + contraseña) para el 16 de septiembre de 2024.
El gigante también anunció el fin del soporte para las aplicaciones 'Correo' y 'Calendario' en Windows, la desactivación de Outlook Light y la eliminación de la capacidad de los usuarios para acceder a cuentas de Gmail a través de Outlook.com.

INFO

EE.UU. prohíbe el software de Kaspersky, citando riesgos para la seguridad nacional

El Bureau of Industry and Security (BIS) del Departamento de Comercio de los Estados Unidos anunció el jueves una prohibición "sin precedentes" que impide a la subsidiaria estadounidense de Kaspersky Lab ofrecer su software de seguridad, tanto directamente como de manera indirecta, en el país. El bloqueo también se extiende a las filiales, subsidiarias y empresas matrices de la compañía de ciberseguridad, dijo el departamento, agregando que la acción se basa en el hecho de que sus operaciones en Estados Unidos representaban un riesgo para la seguridad nacional. La noticia de la prohibición fue reportada por primera vez por Reuters.

Kaspersky en Respuesta

Kaspersky criticó la decisión del Departamento de Comercio, argumentando que ignora las medidas de transparencia implementadas y sugiriendo que estas restricciones podrían perjudicar la cooperación internacional en la lucha contra el cibercrimen. Esta acción de EE.UU. sigue a restricciones similares implementadas por otros países como Alemania y Canadá en los últimos años, reflejando preocupaciones internacionales sobre la seguridad de los productos de ciberseguridad provenientes de Rusia.

Fecha de Publicación: 21/JUN/2024

Objetivos

Como parte de la prohibición, Kaspersky tendrá prohibido vender su software a los consumidores y empresas estadounidenses a partir del 20 de julio. Sin embargo, la compañía todavía puede proporcionar actualizaciones de software y firmas antivirus a los clientes existentes hasta el 29 de septiembre.

INFO

Hospitales de Londres cancelan más de 800 operaciones tras un ataque de ransomware

Resumen

El NHS Inglaterra reportó que varios hospitales en Londres enfrentaron serias consecuencias debido a un ataque de ransomware contra Synnovis, anteriormente conocido como Viapath. Este incidente, vinculado al ransomware Qilin, obligó a cancelar cientos de operaciones y citas programadas. La restauración completa de los sistemas afectados, incluyendo los del Guy's y St Thomas' NHS Foundation Trust y el King's College Hospital NHS Foundation Trust, podría llevar meses. Además, el NHS Blood and Transplant emitió una advertencia sobre una escasez crítica de sangre tipo O en los hospitales de Londres, subrayando la urgencia de donaciones para mantener operativos los procedimientos médicos esenciales.

Ransomware Qilin

El grupo de ransomware Qilin, anteriormente conocido como "Agenda" desde su surgimiento en agosto de 2022, ha atacado a más de 130 empresas, añadiéndolas a su sitio de filtraciones en la dark web. Aunque su actividad fue limitada inicialmente, se intensificó a finales de 2023 con el desarrollo de un cifrador avanzado para Linux, diseñado para atacar máquinas virtuales VMware ESXi. Qilin opera infiltrándose en las redes de las empresas, extrayendo datos sensibles y obteniendo credenciales de administrador antes de desplegar el ransomware para cifrar todos los dispositivos conectados a la red. El sitio web de filtraciones de Qilin, que estuvo fuera de línea, ha vuelto a estar operativo, aunque la pandilla aún no ha reclamado el ataque

Fecha de Publicación: 14/JUN/2024

INFO

Indicator	Indicator Type	Context
6a93e618e467ed13f98819172e24fffa	MD5	File.exe
e90bdaaf5f9ca900133b699f18e4062562148169b29cb4eb37a0577388c22527	SHA256	File.exe
334fd98ab462edc1274fecdb89fb0791	MD5	File.exe
55e070a86b3ef2488d0e58f945f432aca494bfe65c9c4363d739649225efbbd1	SHA256	File.exe
14dec91fdcaab96f51382a43adb84016	MD5	File.exe
37546b811e369547c8bd631fa4399730d3bdaff635e744d83632b74f44f56cf6	SHA256	File.exe
76f860a0e238231c2ac262901ce447e83d840e16fca52018293c6cf611a6807e	SHA256	File.exe
fd7cbadcfca84b38380cf57898d0de2adcdfb9c3d64d17f886e8c5903e416039	SHA256	File.exe
555964b2fed3cced4c75a383dd4b3cf02776dae224f4848dcc03510b1de4dbf4	SHA256	File.elf
Fd7cbadcfca84b38380cf57898d0de2adcdfb9c3d64d17f886e8c5903e416039	SHA256	File.exe
76f860a0e238231c2ac262901ce447e83d840e16fca52018293c6cf611a6807e	SHA256	File.exe
"aac", "apk", "avi" "bat" "cmd", "conf", "crdownload", "csv", "dat", "desktop", "doc", "gif", "gz", "htm", "html", "image", "iso", "jpg", "log", "mp3", "mp4", "ova", "pdf", "png", "sql", "torrent", "url", "xhtml", "xlsm", "zip", zipx"	Extensions	Encryption extensions

LA IMPORTANCIA DE NO DEPENDER DE SOLO UNA CONTRASEÑA

En la era digital actual, la seguridad de la información personal y profesional es crucial. A diario, utilizamos numerosos servicios en línea que requieren autenticación, desde redes sociales y correos electrónicos hasta plataformas bancarias y herramientas de trabajo. A menudo, cometemos el error de utilizar la misma contraseña para múltiples cuentas, subestimando los riesgos que esto conlleva. Este enfoque puede tener consecuencias graves y generalizadas si una de esas cuentas se ve comprometida. Es fundamental no depender de una sola contraseña y adoptar las mejores prácticas para fortalecer nuestra seguridad digital.

DataSec

csirt_datasec@datasec.com.co

+57 310 285 8969