NÚMERO 81 | AGOSTO 2023

NTT DATA
Trusted Global Innovator

Radar

El magazine de ciberseguridad

CIBERSEGURIDAD, OBJETIVO ESTRATÉGICO.

En la era digital en la que vivimos, la ciberseguridad se ha convertido en un objetivo estratégico de vital importancia para individuos, empresas y gobiernos de todo el mundo. A medida que la tecnología avanza y nuestras vidas se vuelven cada vez más dependientes de los sistemas informáticos y las redes interconectadas, aumentan los riesgos asociados con la seguridad de la información y la protección de los datos sensibles. La ciberseguridad ha adquirido una relevancia fundamental y se ha vuelto estratégica, tanto a nivel individual como a nivel global por una serie de razones:

1. En primer lugar, debido al crecimiento exponencial de las amenazas cibernéticas. Los ciberdelincuentes han desarrollado sofisticadas técnicas para infiltrarse en sistemas informáticos y redes, robando información confidencial, dañando la infraestructura digital y causando interrupciones significativas en las operaciones de nuestro día a día. Estos ataques pueden tener consecuencias devastadoras, tanto económicas como también políticas. Desde robos de identidad y fraudes financieros hasta sabotaje de infraestructuras críticas o ciber espionaje y, por ende, los riesgos son múltiples y están en constante evolución. Por lo tanto, se debe prevenir y mitigar estos ataques, salvaguardando los intereses de las organizaciones y las naciones.
2. En segundo lugar, debido al aumento de la interconectividad global. En la actualidad, estamos más conectados que nunca, gracias a la expansión de Internet y las redes digitales. Esto ha generado nuevas oportunidades obviamente para el comercio, la colaboración y la comunicación, pero también ha creado una superficie de ataque más amplia, compleja y dinámica para los ciberdelincuentes. Las organizaciones y los gobiernos dependen cada vez más de las tecnologías de la información y la comunicación para llevar a cabo sus actividades diarias. Por lo tanto, la ciberseguridad se ha convertido en un componente estratégico para proteger la integridad, confidencialidad y disponibilidad de los datos en un entorno tan interconectado a nivel global.
3. En tercer lugar, debido a las implicaciones políticas y geopolíticas. Los ciberataques pueden tener consecuencias más allá del ámbito económico, afectando a la seguridad nacional y a las relaciones internacionales. Los gobiernos y las organizaciones deben proteger sus infraestructuras críticas (redes eléctricas, sistemas de transporte, redes de comunicación, etc.), de posibles ataques cibernéticos que podrían poner en peligro la estabilidad y la seguridad de un país. Además, los actores estatales y no estatales pueden utilizar el ciberespacio como una herramienta para el espionaje, la desinformación y la influencia política. Por lo tanto, la ciberseguridad es necesaria se para proteger los intereses nacionales y garantizar la estabilidad geopolítica.
4. En cuarto lugar, debido a la protección de la privacidad y los derechos individuales. A medida que recopilamos y compartimos cada vez más información personal en línea, es fundamental proteger la privacidad y garantizar que los datos confidenciales no caigan en manos equivocadas. Los individuos tienen derecho a mantener el control sobre su información y a estar protegidos contra el robo de identidad, el acoso en línea y otras formas de abuso en la red. Por lo tanto, la ciberseguridad debe salvaguardar la confianza en el mundo digital y proteger los derechos y libertades fundamentales de las personas.

En resumen, nos encontramos ante un panorama donde la ciberseguridad se encuentra embebida dentro de nuestras vidas tanto en un ámbito personal como profesional resultando ser clave y estratégica en nuestra sociedad digital. El crecimiento de las ciberamenazas, la interconectividad global, las implicaciones políticas y geopolíticas, así como la protección de la privacidad y los derechos individuales, han impulsado la necesidad de priorizarla en el ámbito digital. Es por ello por lo que tanto organizaciones como gobiernos deben invertir en medidas de ciberseguridad efectivas para estar protegido y proteger a los individuos contra los ciberataques y garantizar la confianza y la estabilidad en el mundo digital que se encuentra constante evolución.

Enrique Bernao Rosado

Manager de Ciberseguridad en NTT DATA Europe & Latam

CIBERCRÓNICA

En esta edición hablaremos del auge de los nuevos vectores de entrada que están surgiendo a raíz de la creación de nuevas herramientas basadas en inteligencia artificial y demás innovaciones. Haremos hincapié en las ya conocidas extensiones para navegadores.

Los vectores de entrada en ciberseguridad se refieren a los puntos de acceso a sistemas y redes que pueden ser explotados por ciberdelincuentes para llevar a cabo ataques maliciosos.

Desde la inteligencia artificial, pasando por el blockchain y hasta la computación en la nube, estas innovaciones están transformando sectores enteros y abren un abanico de posibilidades sin precedentes. Sin embargo, junto con el progreso tecnológico también surgen desafíos relacionados con la seguridad.

> "El Instituto Nacional de Ciberseguridad de España advierten de que algunos usuarios malintencionados podrían utilizar ChatGPT con fines delictivos."

Es sonado el auge que la inteligencia artificial ha tenido este año 2023. A raíz de la aparición de ChatGPT están surgiendo multitud de herramientas que utilizan inteligencia artificial (IA en adelante), y entre estas se encuentran las extensiones para navegadores y aplicaciones web que permiten realizar tareas de forma mucho más ágil: búsqueda de información, redacción de textos específicos o retoques fotográficos. Sin embargo, este aumento en la aparición de herramientas supone al mismo tiempo un aumento en el riesgo de que algunas de estas aplicaciones contengan malware que acceda a la información de nuestro dispositivo.

Recientemente, los expertos de seguridad de la empresa Kolide han realizado un estudio en el que se muestra que muchas de estas extensiones IA están pensadas para robar información de los usuarios. Esto no es nuevo, pero existe una tendencia masiva en estos momentos sobre el uso de este tipo de herramientas.

En marzo de 2023, guard.io analizó e informó de una herramienta llamada "Quick access to Chat GPT" la cual estaba secuestrando las cuentas de los usuarios a través de la captación de las cookies de sus navegadores. Google está reaccionando en el caso de su navegador (Google Chrome) para filtrar y eliminar rápidamente estas herramientas de su Marketplace de extensiones, sin embargo, la gran demanda de estas herramientas hace que sea una tarea compleja el detectar todas las aplicaciones malintencionadas que salen nuevas cada día y que se encuentran disponibles para los usuarios.

El riesgo se encuentra también mayoritariamente en que, durante el tiempo que los navegadores tardan en eliminar estas extensiones, una gran cantidad de usuarios pueden estar descargando, instalando y promoviendo el uso de estas herramientas.

Otro aspecto importante es el intento de desarrollar una extensión o herramienta de forma ágil y rápida con la finalidad de llegar primero al mercado. Esto hace que muchas aplicaciones, aunque no se encuentren desarrolladas con mala intención, estas contengan muchas vulnerabilidades de código, ya que en este proceso ágil de desarrollo a veces se suele obviar la cobertura de seguridad, produciendo de este modo gran cantidad de puntos débiles en términos de privacidad.

Dicho esto, es muy importante que, a la hora de añadir una extensión a nuestro navegador, nos aseguremos que la fuente que ha desarrollado esta herramienta sea confiable y que tiene la aprobación de las entidades que la distribuyen.

Si hablamos directamente del uso de ChatGPT, desde el Instituto Nacional de Ciberseguridad de España advierten de que algunos usuarios malintencionados podrían utilizar ChatGPT con fines delictivos, ya que, tal y como sucede con otras herramientas, “existen varios vectores de ataque que los ciberdelincuentes pueden aprovechar para explotar vulnerabilidades y atacar a posibles víctimas”.

Aunque ChatGPT está dotado de protocolos de seguridad que le impiden responder a ciertas solicitudes y preguntas malintencionadas, puede permitir a alguien sin conocimientos técnicos desarrollar scripts y realizar ataques de todo tipo, eludiendo las restricciones existentes. Además, volviendo al tema de las herramientas y extensiones, muchas de estas aplicaciones pueden ayudar al usuario con estos fines; reformulando sus preguntas o realizando pruebas que permitan vulnerar estos controles.

Desde INCIBE señalaron: Apoyándose en la herramienta, los ciberdelincuentes podrían obtener información más específica sobre la empresa a la que quieren atacar. De esta forma, logran hacer el mensaje más creíble y hay más posibilidades de que la víctima “muerda el anzuelo” refiriéndose a ataques de suplantación y phishing.

En resumen, y como sucede cada vez que una nueva tecnología sale al mercado, están apareciendo nuevas vulnerabilidades y vectores de ataque. Esto provocará que se creen nuevos requerimientos de seguridad a la hora de desarrollar, analizar y publicar herramientas que contengan estas tecnologías. Una vez más, una carrera entre los ciberdelincuentes que intentan aprovecharse de las vulnerabilidades y los expertos en ciberseguridad que intentan resguardar a los usuarios de estas.

SEGURIDAD Y MALWARE EN DISPOSITIVOS INTELIGENTES

Por: NTT DATA Europe & Latam

En la era de la tecnología conectada, los dispositivos inteligentes se han vuelto una parte integral de nuestras vidas. Desde teléfonos y relojes inteligentes hasta televisores y electrodomésticos conectados a Internet, estos dispositivos nos ofrecen comodidad y eficiencia en nuestras tareas diarias. Sin embargo, junto con los beneficios que brindan, también existe una preocupación creciente: los dispositivos inteligentes se han convertido en objetivos para los ciberdelincuentes. En este artículo, exploraremos esta preocupación y analizaremos por qué es importante ser conscientes de los riesgos asociados con estos dispositivos.

El auge de los dispositivos inteligentes

El auge de los dispositivos inteligentes ha sido impresionante en los últimos años. La conectividad de los dispositivos ha llevado al auge de tecnologías como el internet de las cosas (IoT, por sus siglas en inglés), que permite que múltiples dispositivos se comuniquen y compartan información entre sí. Esto ha mejorado nuestra forma de vivir, brindándonos mayor control y acceso remoto a nuestras pertenencias y servicios.

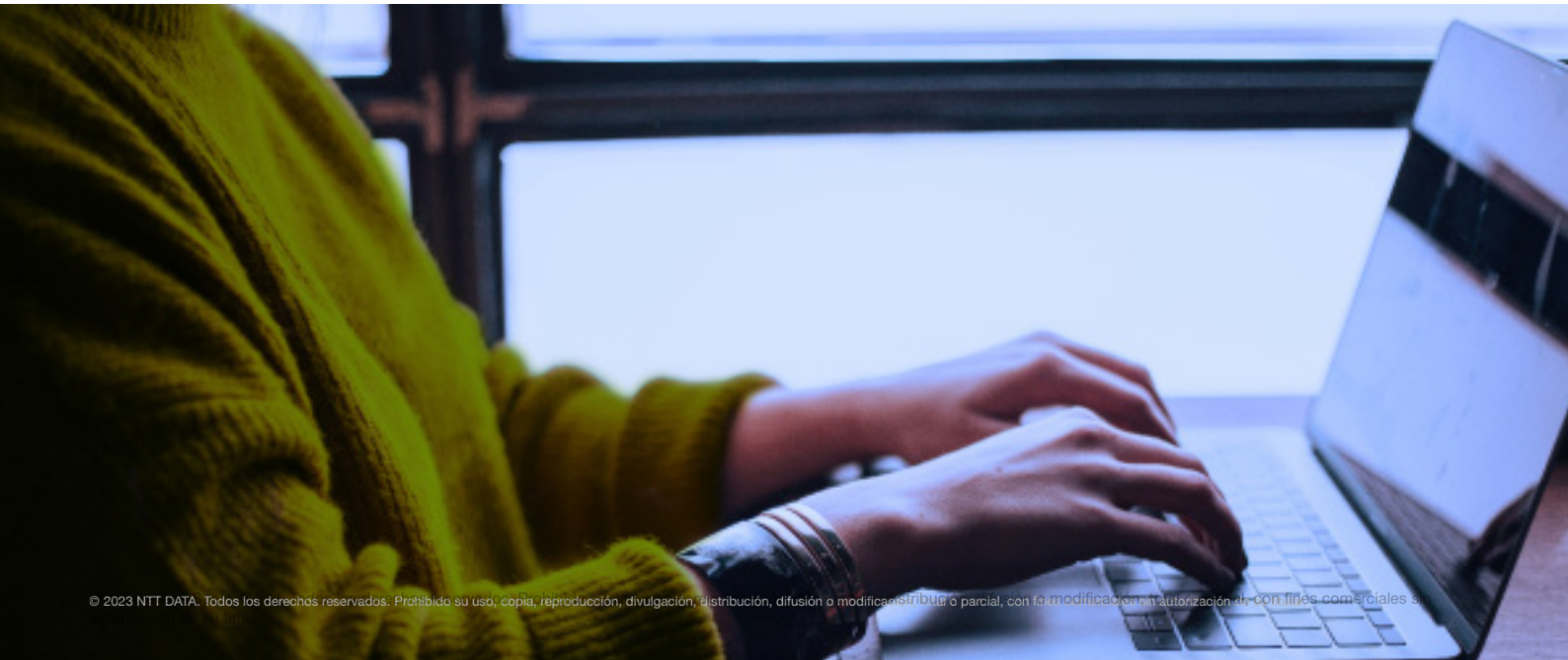
Los riesgos de seguridad

Sin embargo, con la creciente cantidad de dispositivos inteligentes en nuestros hogares y vidas, también hemos visto un aumento en los riesgos de seguridad asociados. Los ciberdelincuentes se aprovechan de las vulnerabilidades presentes en estos dispositivos para acceder a nuestra información personal y financiera, espiar nuestras actividades y, en algunos casos, incluso tomar el control de los dispositivos.

Una de las principales preocupaciones es la falta de seguridad en el diseño y fabricación de estos dispositivos. Muchos fabricantes no prestan suficiente atención a la protección de los datos o la implementación de medidas de seguridad robustas, incumpliendo en algunos casos los estándares de seguridad establecidos. Esto deja a los usuarios expuestos a ataques cibernéticos que podrían tener consecuencias devastadoras.

Además, los dispositivos inteligentes a menudo se conectan a través de redes Wi-Fi, que también pueden ser vulnerables a intrusiones. Las contraseñas débiles o la falta de actualizaciones de seguridad pueden hacer que las redes domésticas sean objetivos fáciles para los ciberdelincuentes.

Esto puede ocasionar que la perdida de información personal muy sensible, desde las ubicaciones y rutas registradas en el GPS, información bancaria o sanitaria… llegando a poder exponer y monitorizar hábitos personales.



Las ultimas estafas conocidas

El regalo con “sorpresa”

Recientemente, se ha detectado un patrón inquietante en el que algunos ciudadanos reciben paquetes sorpresa que contienen dispositivos como auriculares inalámbricos, smartwatches, smart-bands y otros wearables. Sin embargo, detrás de este aparente gesto amable, se esconde un peligroso secreto.

Estos dispositivos contienen malware, un software malicioso diseñado para comprometer la privacidad y seguridad de los usuarios. Una vez que estos dispositivos son vinculados a otros equipos, el malware se activa silenciosamente, permitiendo a los delincuentes acceder a información personal y confidencial, sin el conocimiento ni el consentimiento de los afectados.

Este malware puede acceder tanto a la voz como a las cámaras, lo que permite a los estafadores acceder a conversaciones y cuentas vinculadas a los relojes inteligentes (GPS, métodos de pago y mensajes).

En el caso de recibir un paquete no deseado y que contenga dispositivos electrónicos, las autoridades recomiendan no encenderlos y avisar inmediatamente o entregar el envío a la Policía.

Estos productos también se pueden utilizar para el brushing. Esta es la práctica de enviar productos, a menudo falsificados, no solicitados a personas aparentemente aleatorias por correo para permitir que las empresas escriban reseñas positivas en nombre del destinatario, lo que les permite competir con productos establecidos.

Prevención y consejos

Aunque la seguridad absoluta no existe, hay medidas que los usuarios pueden tomar para protegerse de los ciberdelincuentes. Aquí hay algunos consejos clave:

- Mantén tus dispositivos actualizados: Asegúrate de instalar las actualizaciones de software y firmware más recientes en tus dispositivos inteligentes. Estas actualizaciones suelen contener correcciones de seguridad importantes.
- Contraseñas sólidas: Utiliza contraseñas fuertes y únicas para tus dispositivos y redes Wi-Fi. Evita contraseñas predefinidas o fáciles de adivinar.
- Redes seguras: Configura tu red Wi-Fi doméstica con medidas de seguridad adecuadas, como encriptación WPA2 y un nombre de red único.
- Investigación previa: Antes de comprar un dispositivo inteligente, investiga sobre la reputación del fabricante en cuanto a seguridad y privacidad. Opta por aquellos que se tomen en serio estos aspectos. Comprobando las ubicaciones y estándares de seguridad reconocidos y aplicados por el fabricante
- Protección de datos: Asegúrate de leer y comprender las políticas de privacidad y los términos de servicio de los dispositivos y aplicaciones que utilizas. Considera limitar el acceso a la información personal solo a las funciones necesarias

TENDENCIAS

El auge del Malware en dispositivos móviles y otras preocupaciones

En la era digital actual, los dispositivos móviles se han convertido en una parte integral de nuestras vidas, brindándonos conectividad, comodidad y acceso a una amplia gama de aplicaciones y servicios. Sin embargo, esta creciente dependencia también ha dado lugar a un aumento en los riesgos y amenazas cibernéticas que afectan a los dispositivos móviles.

Los expertos predicen que las amenazas a la seguridad móvil aumentarán drásticamente en 2023. Según un reciente informe de Cybersecurity Ventures, se espera que el número de amenazas a la seguridad móvil aumente más de un 500% en los próximos tres años.

El malware para dispositivos móviles ha evolucionado rápidamente. Habitualmente, los ciberdelincuentes se centraban en la falta de controles de seguridad de los sistemas operativos y en los escasos controles de los mercados de aplicaciones para llevar a cabo actividades maliciosas. Sin embargo, a medida que estas áreas han evolucionado, los actores maliciosos están importando técnicas y tácticas del panorama general de amenazas al mundo de dispositivos móviles.

El fraude, la usurpación de identidad, la interrupción de servicios y el robo de credenciales siguen aumentando a pesar de los esfuerzos de los proveedores de hardware y software en implementar contramedidas ante estos ataques. Esto se debe principalmente a la dificultad de mantener un equilibrio entre lo humano y los sistemas junto con sus procesos. Este factor humano, al ser inherente en estos dispositivos, siempre será el foco de estas actividades maliciosas actuando vector de entrada permitiendo hacer uso de técnicas más sofisticadas pudiendo comprometer, entre otras cosas, las llaves de las identidades digitales almacenadas en el dispositivo móvil.

Por ejemplo, en los últimos años, el malware Pegasus ha sido un tema recurrente en los titulares de noticias y ha causado preocupación en la comunidad de seguridad informática. Desarrollado por la empresa israelí NSO Group, Pegasus es un software espía avanzado diseñado para dispositivos móviles que ha sido utilizado para investigar a periodistas, políticos, activistas de derechos humanos y personas de interés en todo el mundo.

Una de las características más alarmantes de Pegasus es su capacidad para infectar dispositivos sin el factor humano mencionado con anterioridad, aprovechando vulnerabilidades en los sistemas operativos móviles. Una vez que se instala en un dispositivo, el malware es capaz de recopilar información confidencial, como mensajes de texto, correos electrónicos, grabaciones de llamadas, ubicación GPS y contraseñas.

Aunque es difícil controlar este tipo de ciberataques avanzados patrocinados por el Estado, sin duda hay vectores de ataque que pueden detenerse, como el smishing o el malware más habitual en dispositivos móviles. En el amplio ecosistema de aplicaciones móviles, las tiendas oficiales como **Google Play**, han sido tradicionalmente consideradas como lugares seguros y perfectamente confiables para descargar aplicaciones. Sin embargo, en los últimos tiempos, se ha demostrado que no utilizan métodos infalibles para evitar la subida de aplicaciones fraudulentas, existiendo un incremento alarmante de la presencia de malware dentro de estas tiendas.

Recientemente, el malware llamado **Clicker** se infiltró en Google Play haciéndose pasar por herramientas de utilidad como linternas, lectores QR, cámaras, conversores de unidades o gestores de tareas. Este tipo de troyano realiza fraudes publicitarios, mediante conexiones recurrentes a sitios web en segundo plano, permitiendo a los ciberdelincuentes obtener ingresos a través de anuncios y clics. En total, este troyano se habría confirmado en 16 aplicaciones consideradas seguras y disponibles en Google Play sumando más de 20 millones de descargas.

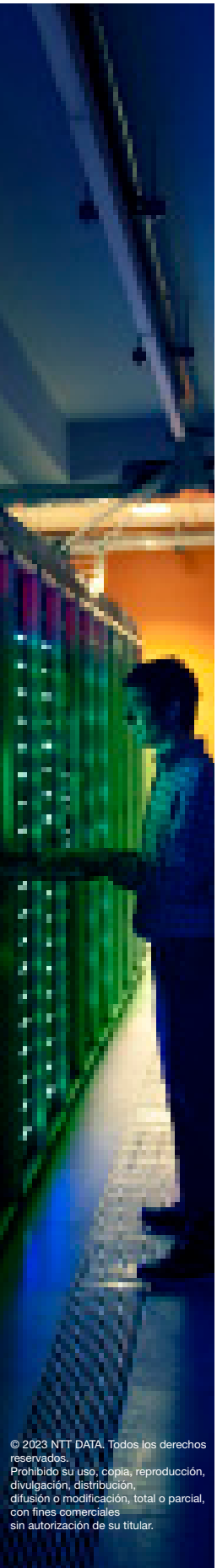
Aunque los usuarios deben ser conscientes de los riesgos potenciales y tomar medidas para proteger sus dispositivos, también es crucial que los desarrolladores sean proactivos a la hora de garantizar la seguridad de sus aplicaciones. Esto puede incluir la aplicación de mejores medidas de seguridad, como la autenticación de dos factores o el cifrado y así mantener a salvo a los usuarios. Además, deberán tener en cuenta siempre este factor humano e intentar implementar medidas adicionales que eviten el mayor daño posible cuando esto falle.

Este aumento de las amenazas a la seguridad móvil se debe al mayor uso de los dispositivos móviles para actividades sensibles, como las operaciones bancarias y compras. Con el paso de los años y las mejoras de este tipo de dispositivos, hay cada vez más personas que utilizan exclusivamente el móvil y carecen de un ordenador personal. Por otro lado, el auge del mundo IoT está aumentando enormemente el potencial de las ciber amenazas dirigidas a los dispositivos móviles dado a que, en sus inicios, eran sistemas que no disponían de apenas seguridad ya que su objetivo era ofrecer este tipo de tecnología al menor coste, siendo la seguridad una de las características donde se recortaba para abaratar costes favoreciendo al desarrollo de múltiples vectores de entrada.

Estas predicciones demuestran la necesidad de aumentar las medidas de seguridad móvil. Por ello, es esencial comprender las amenazas potenciales y tomar medidas para protegerse con la colaboración de usuarios y desarrolladores manteniendo así sus dispositivos seguros y protegidos. Como en cualquier ámbito de la ciberseguridad, la defensa siempre va un paso por detrás del ataque, es por ello por lo que el tapar el mayor número de agujeros posibles que puedan servir de vector de entrada es de vital importancia.

VULNERABILIDADES

Reciba nuestro boletín completo de parches y vulnerabilidades suscribiéndose **aquí**.



Linux

CVE-2023-3269
Fecha: 11/07/2023

Descripción.El pasado 11 de julio se publicó una vulnerabilidad que afecta al subsistema de gestión de memoria del kernel de Linux. La vulnerabilidad ocurre debido a que la gestión de bloqueos para acceder y actualizar áreas de memoria virtual (VMA) es incorrecta, lo que lleva a causar problemas tras liberar la memoria. Esta vulnerabilidad puede ser explotada con éxito para lograr ejecutar código arbitrario del kernel, escalar contenedores y, además, lograr privilegios de root.

Enlace: https://my.f5.com/manage/s/article/K000135446?utm_source=f5support&utm_medium=RSS
https://www.ccn-cert.cni.es/component/vulnerabilidades/view/34489.html
https://www.cve.org/CVERecord?id=CVE-2023-3269

Productos afectados. Kernel de Linux para distribución Fedora, todas las versiones afectadas.

Solución: Actualizar a la versión más reciente.

FortiOS/FortiProxy

CVE-2023-33308
Fecha: 11/07/2023

Descripción. Se ha identificado una vulnerabilidad crítica en FortiOS y FortiProxy. Esta vulnerabilidad de desbordamiento basada en pila permitir a un atacante remoto ejecutar código o comandos arbitrarios a través de paquetes específicamente preparados que alcancen políticas de proxy o políticas de cortafuegos con modo proxy junto con inspección profunda de paquetes SSL. El mismo día en el que se detectó la vulnerabilidad crítica se lanzaron parches de seguridad para poder implementar las correcciones necesarias en FortiOs y FortiProxy.

Enlace: https://www.cisa.gov/news-events/alerts/2023/07/11/fortinet-releases-security-update-fortios-and-fortiproxy
https://www.fortiguard.com/psirt/FG-IR-23-183

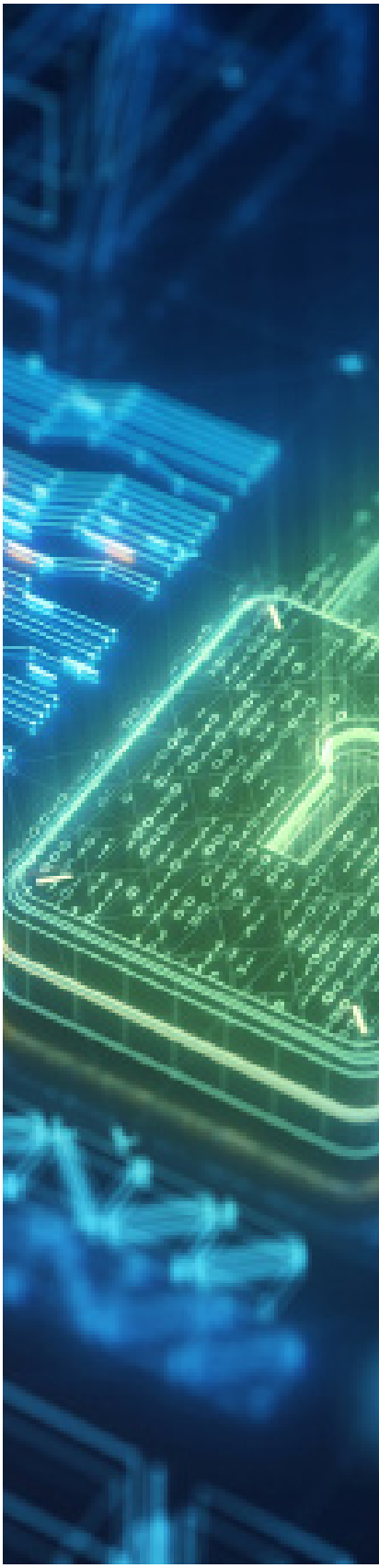
Productos afectados. Los recursos afectados por esta vulnerabilidad son los siguientes:

- FortiOS versión 7.2.0 a 7.2.3.
- FortiOS versión 7.0.0 a 7.0.10.
- FortiProxy versión 7.2.0 a 7.2.2.
- FortiProxy versión 7.0.0 a 7.0.9.

Solución: Desde el fabricante se han proporcionado los siguientes parches:

- Actualizar a FortiOS versión 7.2.4 o superior.
- Actualizar a FortiOS versión 7.0.11 o superior.
- Actualizar a FortiProxy versión 7.2.3 o superior.
- Actualizar a FortiProxy versión 7.0.10 o superior.

PARCHES



Adobe

Fecha: 11-07-2023

Descripción. Adobe ha publicado una actualización de seguridad para Adobe ColdFusion para solventar vulnerabilidades críticas y altas encontradas en abril de 2023.
Las vulnerabilidades de seguridad crítica se detallan a continuación:
• CVE-2023-29298: bypass del control de acceso en el que se permite el paso a diferentes rutas de administrador desde orígenes no autorizados.
• CVE-2023-29300: deserialización de datos no fiables que acaba produciendo ejecución arbitraria de código.
• CVE-2023-29301: vulnerabilidad relacionada con poca restricción o intentos excesivos de autenticación.

Enlace:
https://www.zerodayinitiative.com/blog/2023/7/10/the-july-2023-security-update-review
https://helpx.adobe.com/security/products/coldfusion/apsb23-40.html

Productos afectados:
• ColdFusion 2018: actualización 16 y versiones anteriores.
• ColdFusion 2021: actualización 16 y versiones anteriores.
• ColdFusion 2023: GA Release (2023.0.0.330468).

Solución:
• ColdFusion 2018: actualización 17.
• ColdFusion 2021: actualización 17.
• ColdFusion 2023: actualización 1.

Microsoft

Fecha: 06-06-2023

Descripción. El pasado 11 de julio se publicaron múltiples vulnerabilidades 0-day que actualmente son explotables en productos de Microsoft. CVE-2023-32046: vulnerabilidad de elevación de privilegios en la plataforma Windows MSHTML. Esta vulnerabilidad se explotaba abriendo un archivo especialmente diseñado a través de correo electrónico o sitios web maliciosos. CVE-2023-32049: vulnerabilidad de elusión de funciones de seguridad de Windows SmartScreen. CVE-2023-36874: vulnerabilidad de elevación de privilegios en el servicio de notificación de errores de Windows: este fallo de elevación de privilegios activamente explotado permitía a los actores de amenazas obtener privilegios de administrador en el dispositivo Windows. CVE-2023-36884: vulnerabilidad de ejecución remota de código HTML en Office y Windows: Microsoft ha publicado una guía sobre un 0-day de Microsoft Office y Windows no parcheado y divulgado públicamente que permite la ejecución remota de código utilizando documentos de Microsoft Office especialmente diseñados. CVE-2023-35311: vulnerabilidad de elusión de funciones de seguridad de Microsoft Outlook: vulnerabilidad de 0-day explotada activamente en Microsoft Outlook que elude las advertencias de seguridad y funciona en el panel de vista previa. CVE-2023-32057: vulnerabilidad de ejecución remota de código en colas de mensajes de Microsoft.
Además de las vulnerabilidades 0-day se han encontrado la siguiente cantidad de vulnerabilidades en productos de Microsoft:
• 33 vulnerabilidades de elevación de privilegios
• 13 vulnerabilidades de elusión de funciones de seguridad
• 37 vulnerabilidades de ejecución remota de código
• 19 vulnerabilidades de divulgación de información
• 22 vulnerabilidades de denegación de servicio
• 7 vulnerabilidades de suplantación de identidad

Enlace: https://www.zerodayinitiative.com/blog/2023/7/10/the-july-2023-security-update-review
https://www.bleepingcomputer.com/news/microsoft/microsoft-july-2023-patch-tuesday-warns-of-6-zero-days-132-flaws/

Productos afectados: Múltiples productos de Microsoft.

Solución: Actualizar con los parches indicados para cada producto de Microsoft.último parche de seguridad de junio 2023.

EVENTOS

Cybersecurity Summer BootCamp

03 - 13 de julio de 2023 |

El Instituto Nacional de Ciberseguridad (INCIBE) y la Organización de los Estados Americanos (OEA) organizan anualmente el Cybersecurity Summer BootCamp, un programa internacional de capacitación especializado en ciberseguridad dirigido a Fuerzas y Cuerpos de Seguridad, Ministerio Fiscal, Jueces y Magistrados, Formuladores de políticas y Especialistas de Centros de Respuesta a Incidentes Cibernéticos.

Enlace: https://www.incibe.es/eventos/summer-bootcamp

Congreso de Transformación Digital del Tercer Sector Social de Cataluña

11 de julio de 2023 |

El próximo 11 de julio, desde la Taula d'entitats del Tercer Sector Social de Catalunya, a través del proyecto m4Social y con colaboración con la Fundación Telefónica, se organiza el 'Congreso de Transformación Digital del Tercer Sector Social de Cataluña' en el Hub Social (c/ Girona, 34, 08010 – Barcelona).

Enlace: https://m4social.org/es/esdeveniment/congres-de-transformacio-digital-del-tercer-sector-social-de-catalunya/

Cybersecurity Financial & Government Edición Ecuador

6 de julio 2023 |

Cybersecurity Financial & Government Edición Ecuador se celebra en Swissotel Quito el 6 de 2023 mostrando la actualidad empresarial de Ecuador e internacional relacionada con los sectores Tecnologías digitales, Tecnología de seguridad.

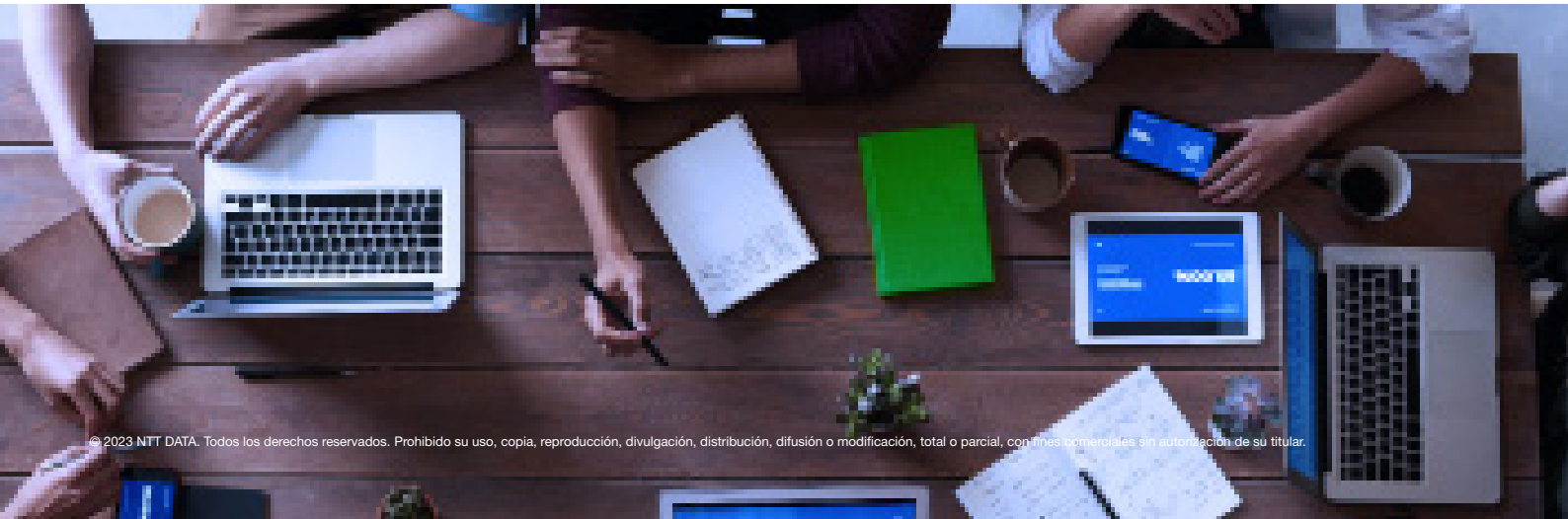
Enlace: https://www.neventum.es/ferias/cybersecurity-financial-government-edicion-ecuador

Cyber Security EXPO

5 - 10 de abril de 2023 |

La EXPO de Ciberseguridad es el único evento dedicado a la contratación diseñado para clientes y agencias de contratación que operan en el sector de la ciberseguridad. Debido a la naturaleza sensible de algunos puestos de trabajo y al hecho de que es posible que los candidatos deseen mantener la discreción.

Enlace: https://www.cybersecurityexpo.co.uk/manchester



RECURSOS

RULES_OCI CON BAZEL

Google ha lanzado recientemente Rules_oci, una extensión de código abierto para Bazel que tiene como objetivo facilitar y mejorar la seguridad en la creación de imágenes de contenedores. Este complemento, conocido como un "conjunto de reglas", ofrece soporte tanto a la comunidad de contenedores como a la seguridad de las imágenes de contenedores.

Enlace: https://noticiasseguridad.com/tutoriales/proteger-las-imagenes-de-los-contenedores-con-la-herramienta-gratis-de-google-rules_oci-con-bazel/

Cisco anuncia Extended Detection and Response (XDR)

Cisco está desarrollando una solución XDR que combina la experiencia en redes y terminales para una detección y respuesta basada en riesgos. Cisco XDR, en fase beta, estará disponible en julio de 2023. La solución cloud nativa aplica analítica para priorizar detecciones y automatizar la respuesta, reduciendo investigaciones interminables en los centros de operaciones de seguridad.

Enlace: https://bitlifemedia.com/2023/05/cisco-presenta-nuevas-soluciones-ciberseguridad-xdr/

Google Cloud combate el blanqueo de capitales en entidades financieras con IA

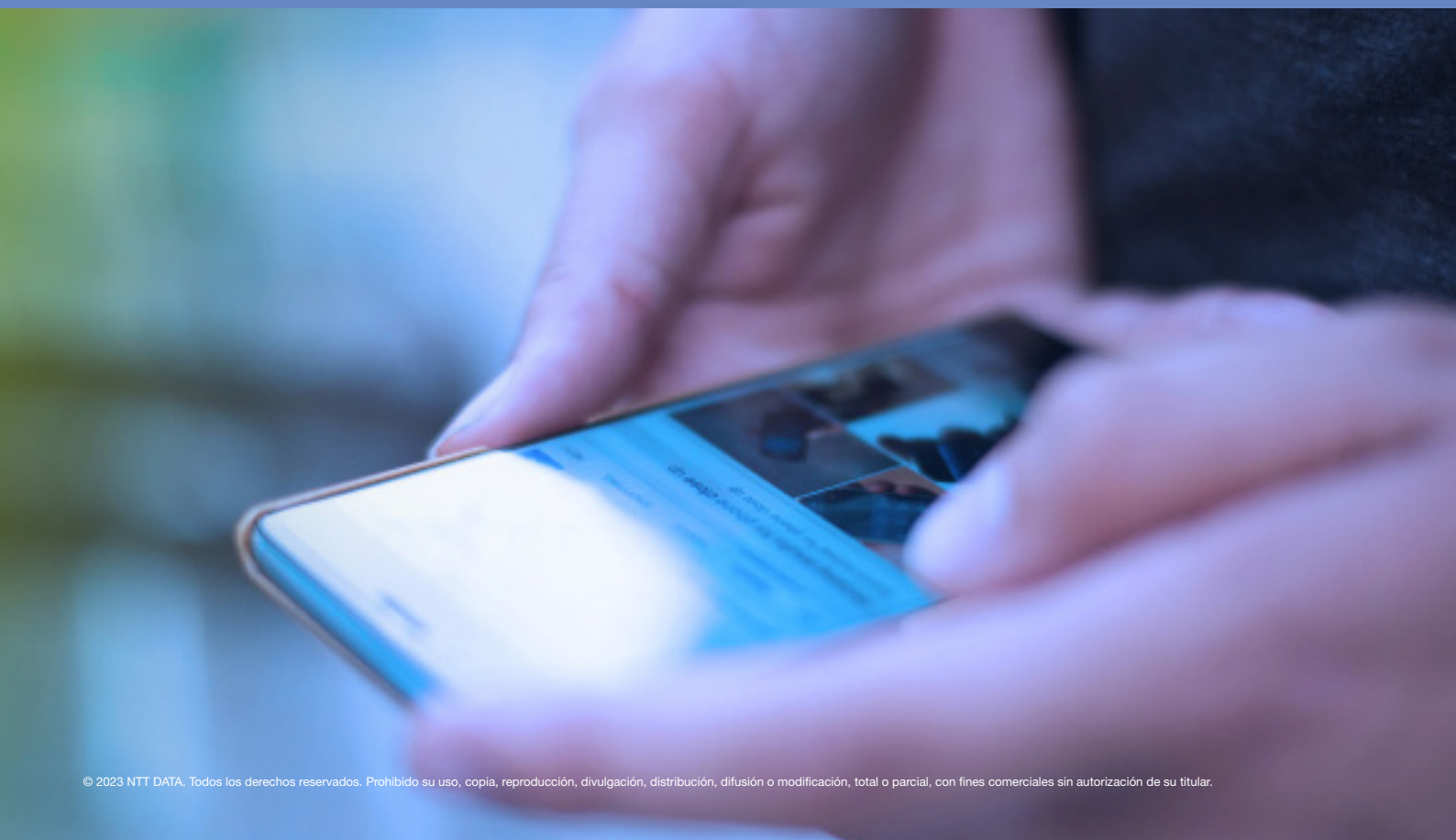
Google Cloud ha presentado AML AI (Anti Money Laundering AI), un producto impulsado por inteligencia artificial (IA) que tiene como objetivo mejorar la detección del blanqueo de capitales en entidades financieras. Esta solución, diseñada específicamente para combatir este tipo de delito de manera más eficaz y eficiente, aprovecha la potencia de la IA para ofrecer análisis avanzados y precisos. Con AML AI, las entidades financieras pueden fortalecer su capacidad de detectar y prevenir actividades ilícitas relacionadas con el blanqueo de capitales, brindando una mayor protección y seguridad en su operativa.

Enlace: https://cybersecuritynews.es/google-cloud-lanza-un-producto-para-luchar-contra-el-blanqueo-de-capitales-asistido-por-ia-para-entidades-financieras/

Nuevo método de phishing detectado en Microsoft Teams: Suplantación de usuarios internos y envío de mensajes fraudulentos

Se ha descubierto un nuevo método de phishing en la aplicación de Microsoft Teams, el cual permite a los atacantes suplantar a usuarios internos de una organización y enviar mensajes engañosos a otros usuarios. Como resultado de esto, el investigador de seguridad Alex Reid ha creado una herramienta llamada "TeamsPhisher" utilizando Python, la cual automatiza por completo este tipo de ataque. El software combina las estrategias de ataque desarrolladas por los investigadores de Jumpsec, las técnicas de Andrea Santese, y las funciones de autenticación y asistencia de la herramienta "TeamsEnum" creada por Bastian Kanbach.

Enlace: https://github.com/Octoberfest7/TeamsPhisher




NTT DATA
Trusted Global Innovator
powered by the
cybersecurity NTT DATA team
nttdata.com