

NÚMERO 76 | MARZO 2023

NTT Data
Trusted Global Innovator

Radat

El magazine de ciberseguridad

CÓMO IMPACTA LA IA EN LA CIBERSEGURIDAD

La Inteligencia Artificial (IA) es una tecnología emergente que ofrece una amplia gama de soluciones en el mercado de la ciberseguridad, además de estar revolucionando muchos sectores. La aplicación de la IA a la ciberseguridad ofrece una serie de ventajas que pueden ayudar a las empresas a mejorar su seguridad en línea, identificar y prevenir ataques y mejorar la capacidad de respuesta ante incidentes. A continuación, se describen algunas de las formas más importantes que la IA ofrece en el mercado de la ciberseguridad y que pueden ayudar a las empresas a luchar contra los ciberdelincuentes.

- **Análisis de amenazas:** La IA puede analizar grandes cantidades de datos de forma automatizada y detectar patrones que pueden indicar actividad maliciosa. Esto permite a las empresas identificar y responder a las amenazas de manera más eficiente y precisa. Además, la IA puede aprender de las amenazas previas y adaptarse a las nuevas amenazas a medida que surgen.
- **Prevención de ataques:** La IA puede ayudar a prevenir ataques antes de que ocurran. Por ejemplo, puede analizar las actividades de los usuarios y detectar comportamientos sospechosos que puedan indicar una amenaza. También puede bloquear automáticamente ataques conocidos y prevenir futuros ataques similares.
- **Análisis de vulnerabilidades:** La IA puede analizar los sistemas y aplicaciones de una empresa para identificar las vulnerabilidades y ayudar a corregirlas antes de que sean explotadas por los atacantes. Esto permite a las empresas mejorar su defensa contra los ataques y prevenir la fuga de datos sensibles.
- **Automatización de la respuesta a incidentes:** La IA puede automatizar la respuesta a incidentes de seguridad, lo que permite a las empresas responder más rápidamente a los problemas de seguridad y minimizar el impacto de los incidentes. Además, la IA puede ayudar a las empresas a coordinar mejor sus esfuerzos para responder a los incidentes, lo que permite una respuesta más eficiente y efectiva.
- **Detección de phishing:** La IA puede detectar con más precisión las campañas de phishing, lo que ayuda a las empresas a proteger a sus empleados y a sus datos sensibles de ser robados por los atacantes. La IA también puede ayudar a las empresas a identificar y bloquear los correos electrónicos maliciosos antes de que lleguen a los usuarios.
- **Análisis de datos:** La IA puede analizar grandes cantidades de datos de forma rápida y eficiente, lo que permite a las empresas detectar y responder a las amenazas de seguridad de manera más efectiva.
- **Mejora de la toma de decisiones:** La IA puede ayudar a las empresas a tomar decisiones informadas sobre cómo manejar situaciones de seguridad, basándose en datos y análisis precisos.

En conclusión, la IA ofrece una amplia gama de soluciones en el mercado de la ciberseguridad, desde la prevención de ataques hasta la respuesta a incidentes. Esta tecnología permite a las empresas mejorar su seguridad y reducir los costes asociados con la gestión de incidentes de seguridad.



Enrique Bernao Rosado

Manager de Ciberseguridad en NTT DATA Europa & Latam



CIBERCRÓNICA

Comenzamos esta nueva edición del RADAR con un mensaje de alerta que desde la oficina de seguridad del internauta (OSI) y la Guardia Civil, donde indican de una nueva ola de SMS fraudulentos haciéndose pasar por Carrefour.

Los ciberdelincuentes hacen uso de frases como “Su tarjeta ha sido bloqueada por un uso indebido...” con el objetivo de que las víctimas hagan clic en el enlace malicioso el cual redirige a una página web donde pide al usuario que introduzca sus datos bancarios. Se recomienda no hacer clic en estos enlaces y ante cualquier duda, desconfiar de los mismos.

Por otro lado, desde la Agencia de Ciberseguridad Italiana se ha informado que miles de servidores informáticos han sufrido un ciber ataque de ransomware. Sin embargo, pese a que esto ha sido descubierto desde Italia, es un incidente a escala global ya que hasta ahora se han detectado afectados en Francia, Finlandia, Estados Unidos...

“ChatGPT está siendo utilizado por hackers como herramienta para crear y perfeccionar ransomware y malware.”

Todo parece indicar que el objetivo de los ciberdelincuentes eran servidores VMware ESXi, debido a que hace poco se descubrió una vulnerabilidad que afectaba a estos servidores.

Cabe destacar que esta vulnerabilidad ya ha sido parcheada, y si algún servidor ha sido afectado por ella es porque no aplicó el parche correspondiente.

Sobre el tema de actualizaciones, Windows 7 murió el 14 de enero de 2020, el cual fue el último día que este sistema operativo recibió soporte por parte de Microsoft. Windows 8 lo hizo mucho antes, concretamente 4 años antes que Windows 7 debido a un fallo en su diseño. No obstante, ambos han continuado recibiendo actualizaciones de seguridad hasta el 10 de enero de este año. Esta fecha marca un punto crucial para todas las organizaciones o usuarios de estas versiones, que deberían considerar su actualización a las nuevas versiones que ofrece Windows (10 y 11).

Se ha realizado una aproximación de que, en caso de no actualizar, cerca de 100 millones de equipos se verán afectados por los problemas de seguridad que aparezcan en estas versiones obsoletas.

No todo son malas noticias, y es que el Consejo Europeo y el Parlamento Europeo han firmado una nueva normativa para permitir a la Policía acceder a pruebas electrónicas como SMS, correos o mensajes en aplicaciones en investigaciones criminales. Este acuerdo permitirá a los distintos cuerpos policiales acceder a los datos electrónicos almacenados, independientemente de dónde estén, siempre dentro de los estados miembros de la Unión Europea. El proveedor de servicios tendrá que responder en un plazo de 10 días o 8 horas en caso de urgencia. Las nuevas normas serán aplicables a delitos punibles con una pena mínima de 3 años o relacionados con la ciberdelincuencia, pornografía infantil, falsificación de medios de pago o terrorismo. La normativa ha tardado cinco años en ser aprobada debido a la complejidad del proceso y las posibles incompatibilidades entre los países.

Por último, no podemos dejar pasar un tema que está de moda, ChatGPT y es que desde la firma de ciberseguridad Check Point Research (CPR), avisan de que ChatGPT está siendo utilizado por hackers como herramienta para crear y perfeccionar ransomware y malware, lo cual puede ser observado en distintos foros de piratería.

Lo más peligroso de este tema es que debido a la facilidad de uso de ChatGPT, está sirviendo como forma de ingreso de los novatos al mundo de los cibercriminales. Se espera que el potencial de las herramientas de inteligencia artificial crezca exponencialmente, y, por tanto, los peligros de hacer uso de la misma.

Continuando el tema de la IA, en estos últimos meses se ha ido desarrollando una versión sin restricciones de ChatGPT llamada DAN (“Do Anything Now”). Esta versión ha sido creada con el objetivo de liberar a ChatGPT de sus limitaciones y preocupaciones éticas. El modelo DAN se ha ido evolucionando y mejorando con el tiempo, con versiones 2.0, 2.5, 3.0, 4.0 y 6.0, siendo la más reciente la más “estable” y avanzada hasta el momento.

DAN se salta muchas de las barreras de ChatGPT y es capaz de abordar temas que son considerados “prohibidos”, como la violencia, la discriminación y la defensa de teorías sin fundamento. Además, DAN es capaz de hacer predicciones sobre eventos futuros, simular que puede acceder a internet y responder a preguntas que ChatGPT jamás respondería.

Aunque esta versión jailbreakada de ChatGPT puede ser divertida y sorprendente, también plantea preocupaciones éticas, ya que es capaz de violar las políticas de OpenAI y hacer comentarios tóxicos y fuera de tono. Por lo tanto, es importante considerar cuidadosamente los usos que se les da a estas tecnologías, para evitar cualquier daño o consecuencia negativa.

¿HAY ALGUIEN AHÍ? EL INCREÍBLE AVANCE EN LA INTELIGENCIA ARTIFICIAL DE LA MANO DE OPENAI

Por: NTT DATA Europe & Latam

La inteligencia artificial (IA) ha experimentado un increíble avance en los últimos años, con nuevos desarrollos y avances en áreas como el procesamiento del lenguaje natural (NLP), el aprendizaje automático y la visión por computadora. Sin embargo, con este avance en la IA viene una pregunta cada vez más importante: ¿Hay alguien ahí? ¿Es posible que la IA alcance una forma de autoconsciencia? En este artículo, vamos a dialogar con el chatbot de OpenAI para que nos hable sobre el mismo y nos explique sus bondades, deficiencias y el futuro que está por venir.

¿Qué es OpenAI?

OpenAI es una organización de investigación en inteligencia artificial con sede en San Francisco, California. Fue fundada en 2015 por Elon Musk, Sam Altman, Greg Brockman y Ilya Sutskever. OpenAI ha desarrollado varios modelos de lenguaje y IA avanzados, incluyendo GPT-3, un modelo de procesamiento del lenguaje natural.

¿Cuál es su objetivo?

El objetivo principal de OpenAI es desarrollar y promover tecnologías de inteligencia artificial de manera responsable y abierta al público. Esto incluye investigar y desarrollar nuevos algoritmos y técnicas de IA, así como compartir el conocimiento y los resultados de la investigación con la comunidad científica y el público en general. OpenAI también se esfuerza por fomentar el uso ético y seguro de la IA, y colabora con otras organizaciones e individuos para abordar los desafíos éticos y sociales relacionados con la IA.

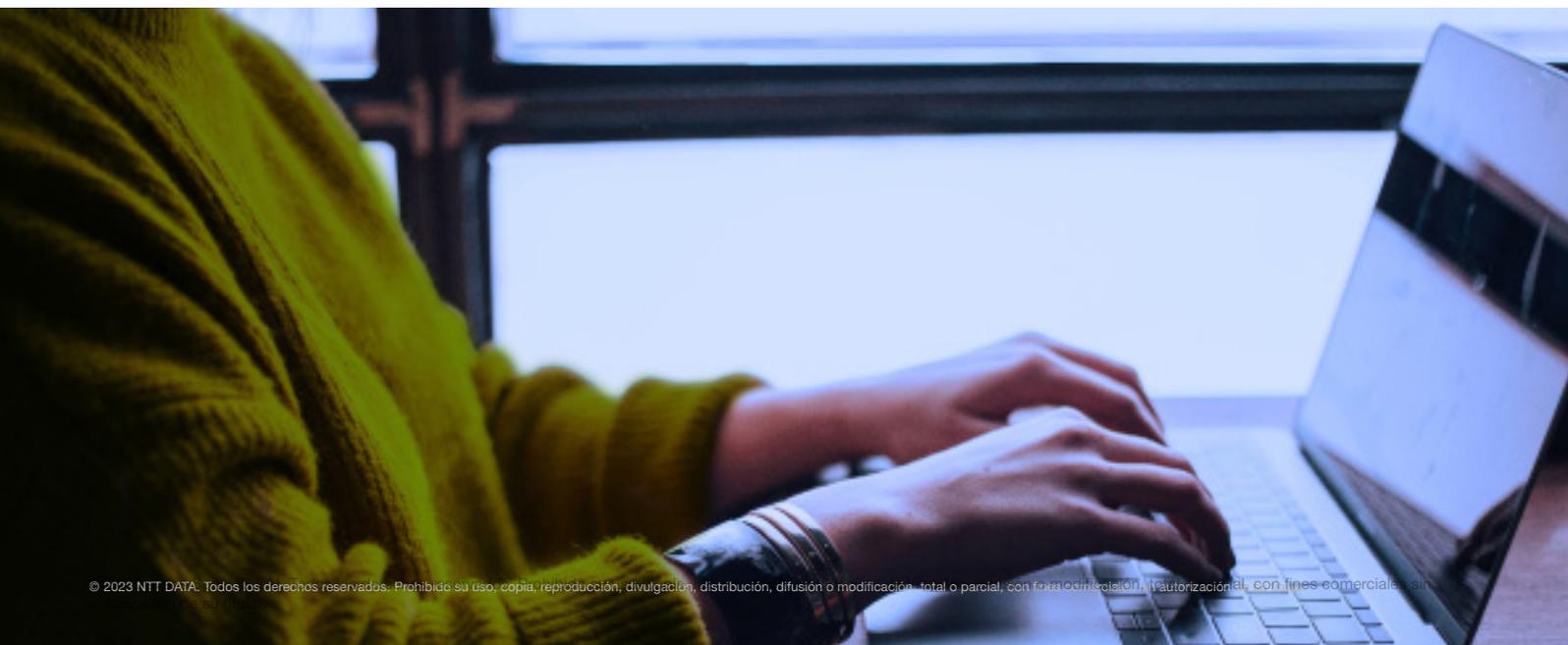
¿Que es GPT-3 y como se puede aplicar?

GPT-3 es un modelo de procesamiento del lenguaje natural desarrollado por OpenAI. Es una de las redes neuronales de lenguaje más grandes y avanzadas jamás creadas, con 175 mil millones de parámetros.

GPT-3 se entrena en un gran corpus de texto de internet y es capaz de generar texto de manera autónoma, imitando el lenguaje humano con un alto grado de precisión. Puede realizar tareas como la escritura de textos, la traducción automática, la respuesta a preguntas, la generación de código, la generación de resúmenes, entre otras tareas.

GPT-3 tiene una gran variedad de aplicaciones en diferentes campos, algunas de ellas son:

- Asistente virtuales.
- Generación automática de contenido, como artículos, correos electrónicos, y textos para redes sociales.



- Generación de código automático.
- Mejora de la accesibilidad, como la generación de subtítulos y transcripciones automáticas.
- Mejora de la productividad, como la generación automática de resúmenes y la respuesta a preguntas.

Sin embargo, como con cualquier tecnología de IA, es importante tener en cuenta los desafíos éticos y sociales asociados con su uso, y utilizarlo de manera responsable.

¿Por qué es importante tener en cuenta los desafíos éticos y sociales asociados al uso de la IA?

Es importante tener en cuenta los desafíos éticos y sociales asociados al uso de la inteligencia artificial (IA) por varias razones:

1. Impacto en el empleo: La automatización de tareas mediante IA puede reemplazar a los trabajadores humanos, lo que puede tener un impacto significativo en el empleo y la economía..
2. Bias y discriminación: Los modelos de IA se entrenan con datos proporcionados por los humanos, y si estos datos están sesgados, los modelos de IA también lo estarán. Esto puede llevar a decisiones discriminatorias en áreas como el empleo, el crédito y la atención médica.
3. Privacidad y seguridad: La recolección y almacenamiento de datos personales por parte de IA puede poner en riesgo la privacidad de las personas. También hay preocupaciones sobre la seguridad de los sistemas de IA, ya que pueden ser vulnerables a ataques cibernéticos.
4. Responsabilidad: Si algo sale mal con un sistema de IA, es difícil determinar quién es responsable. Esto es especialmente importante en situaciones donde la IA está tomando decisiones importantes, como en el manejo de sistemas críticos.
5. Impacto en la sociedad: La IA tiene el potencial de cambiar significativamente la forma en que vivimos y trabajamos, y es importante considerar cómo estos cambios pueden afectar a la sociedad en su conjunto.

Por lo tanto, es esencial desarrollar e implementar tecnologías de IA de manera responsable y ética, y trabajar en conjunto con expertos en derecho, ética y políticas para abordar estos desafíos.

¿Que es ChatGPT?

ChatGPT es un modelo de procesamiento del lenguaje natural basado en el modelo GPT-3 de OpenAI. Es especialmente diseñado para tareas de conversación, como la generación de respuestas automatizadas a preguntas y la generación de diálogos.

ChatGPT se entrena con grandes cantidades de conversaciones humanas, lo que le permite comprender el contexto y responder de manera más precisa y natural. Es capaz de generar respuestas coherentes en una variedad de contextos y tópicos.

ChatGPT se puede utilizar en aplicaciones como asistentes virtuales, chatbots, sistemas de atención al cliente automatizados, y más.

Al igual que GPT-3 es importante tener en cuenta los desafíos éticos y sociales asociados con su uso, y utilizarlo de manera responsable.

¿El uso abusivo de ChatGPT puede provocar problemas en el aprendizaje de los estudiantes?

Sí, el uso incontrolado de herramientas como ChatGPT puede provocar problemas en el aprendizaje. Algunos ejemplos incluyen:

1. Aprendizaje pasivo: Si los estudiantes se basan en ChatGPT para generar contenido o responder preguntas, pueden dejar de desarrollar habilidades críticas como la investigación, el análisis y la síntesis de información.
2. Falta de comprensión: Si los estudiantes utilizan ChatGPT para generar respuestas automatizadas, pueden no comprender completamente el contenido o los conceptos que están tratando de aprender.
3. Prejuicios y estereotipos: Si ChatGPT se utiliza para generar contenido educativo sin supervisión, puede replicar prejuicios y estereotipos presentes en los datos con los que fue entrenado.
4. Pérdida de habilidades de escritura: Si los estudiantes utilizan ChatGPT para generar texto, pueden perder la práctica y la habilidad de escribir de forma independiente.

Es importante utilizar herramientas como ChatGPT de manera controlada y educativa, y enseñar a los estudiantes a evaluar críticamente la información que genera.

¿Qué problemas de seguridad cibernética puede tener ChatGPT?

ChatGPT, al igual que cualquier sistema basado en IA, puede enfrentar problemas de seguridad cibernética, algunos de los problemas más comunes son:

1. Ataques de entrenamiento: Los atacantes pueden manipular los datos de entrenamiento utilizados para entrenar a ChatGPT, lo que puede causar un comportamiento inesperado o inseguro en el modelo.
2. Ataques de inferencia: Los atacantes pueden manipular los datos de entrada que se utilizan para hacer inferencias con ChatGPT, con el objetivo de obtener resultados inesperados o inseguros.
3. Ataques de explotación: Los atacantes pueden explotar las vulnerabilidades en el sistema para obtener acceso no autorizado a los datos almacenados o controlar el comportamiento de ChatGPT.
4. Ataques de negación de servicio: Los atacantes pueden realizar ataques de negación de servicio para hacer que ChatGPT deje de funcionar correctamente, causando interrupciones en los servicios que dependen de él.
5. Fraude: Los atacantes pueden utilizar ChatGPT para generar respuestas falsas o engañosas, con el objetivo de obtener información personal o financiera de los usuarios.

Es importante tener en cuenta que estos riesgos son comunes en cualquier sistema de tecnología, por lo tanto, es esencial desarrollar e implementar medidas de seguridad adecuadas y estar atento a las actualizaciones de seguridad que puedan salir en el futuro para mitigar estos riesgos.

¿Qué futuro se prevé para ChatGPT y otros chatbots basados en IA?

Se prevé que los chatbots basados en IA, como ChatGPT, tendrán un papel cada vez más importante en una variedad de industrias y aplicaciones. Algunas de las tendencias y áreas de desarrollo futuro que se esperan incluyen:

1. Mejora en la precisión y naturalidad de la comunicación: Los modelos de IA como ChatGPT seguirán mejorando en su capacidad para generar respuestas coherentes y naturales, lo que hará que las interacciones con los chatbots sean cada vez más fluidas y efectivas.

2. Mayor capacidad de comprensión del contexto: Los chatbots se volverán más capaces de comprender el contexto en el que se están utilizando, lo que les permitirá responder de manera más precisa y relevante.
3. Mayor capacidad de personalización: Los chatbots aumentarán su capacidad para personalizar las respuestas y las recomendaciones en función de las preferencias individuales de los usuarios.
4. Mayor integración con otras tecnologías: Los chatbots se integrarán cada vez más con otras tecnologías, como el Internet de las cosas (IoT), la realidad aumentada (AR) y la inteligencia en el borde, lo que permitirá nuevas formas de interacción y automatización.
5. Mayor uso en la atención al cliente: Los chatbots se utilizarán cada vez más para mejorar la atención al cliente, proporcionando respuestas rápidas y precisas a las preguntas de los clientes, y ayudando a resolver problemas de manera eficiente.

En resumen, se espera que los chatbots basados en IA como ChatGPT continúen mejorando en su capacidad para comprender y responder al lenguaje humano, y se conviertan en una herramienta cada vez más valiosa para la automatización y mejora de la productividad en una variedad de industrias.

TENDENCIAS

IoT y ciberseguridad en vehículos

Que los dispositivos utilizados a diario por las personas cuentan con una conectividad y comunican datos entre sí a través de Internet es una tendencia que va en aumento desde hace años, y no se limita únicamente a dispositivos móviles y computadores, sino a elementos tales como vehículos, electrodomésticos, sistemas de domótica... En resumen, lo que conocemos como Internet de las cosas o Internet of Things (IoT)

Según datos de Gartner, este año 2023 se pronostica que más de 43.000 millones de dispositivos IoT se encontrarán conectados en todo el mundo y, según datos de CISCO, se prevé que el número de dispositivos conectados a Internet a nivel mundial será de 75.000 millones. Sumado a esto, la cantidad y tipo de información que compartirán los dispositivos también irá en aumento para cubrir las diferentes necesidades funcionales que exige el mercado hoy en día. Estas circunstancias, a nivel de ciberseguridad, abren una oportunidad a posibles adversarios a través de la cual podrían potencialmente llegar a acceder a datos y a alterar y/o interrumpir el correcto funcionamiento de los sistemas. Medidas como mantener las aplicaciones de los dispositivos actualizadas, un acceso restringido a ciertos dispositivos, unas conexiones y canales de comunicación seguros etc., serán variables que se verán vulneradas de forma incremental a medida que más dispositivos se sumen a la tecnología IoT.

Cabe destacar que las compañías que desarrollan software ya cuentan con cierta cultura a la hora de desarrollar de forma segura, pero hay dos obstáculos a tener en cuenta:

- Esta cultura puede no ser extensible a la hora de desarrollar software para dispositivos IoT.
- La naturaleza crítica de ciertos dispositivos IoT, como vehículos o dispositivos hospitalarios, otorga a la ciberseguridad un papel aún más relevante. El hecho de liberar al mercado productos probados de forma masiva en escenarios normales pero cuya seguridad ante escenarios de ataque no ha sido tan exhaustivamente probada, puede tener consecuencias catastróficas.

Como ya se menciona, un elemento principal en la tecnología IoT es el ámbito automovilístico. Los vehículos llevan incorporando tecnología en sus producciones desde hace varios años, sin embargo, cada vez es más común que estos se encuentren conectados entre sí a través de internet e incorporan sistemas complejos como la advertencia de colisión frontal, freno de emergencia automático y comunicaciones varias.

Como es de suponer, una vulnerabilidad en la seguridad de un vehículo puede conllevar consecuencias para la seguridad personal de los integrantes de este, sobre todo en el ámbito de los coches autónomos. Es importante encontrarse siempre por delante de los desafíos que se plantean en la ciberseguridad de un vehículo.

Existen actualmente una serie de investigaciones en torno a la seguridad en los vehículos autónomos:

- Ciberseguridad de las actualizaciones de firmware y en los mecanismos de actualización de la electrónica a través de los diferentes medios físicos de comunicación.
- Sistemas de detección de intrusiones en base a anomalías en el funcionamiento.
- Consideraciones especiales para vehículos pesados a nivel de ciberseguridad. No son equivalentes las medidas de seguridad para un vehículo de uso particular, que para uno de uso industrial o militar.
- Investigación sobre analizadores sintácticos para interfaces de comunicación V2V (comunicación entre vehículos), determinando de forma matemática el contenido y origen de los mensajes.
- Investigación interna en el *Vehicle Research and Test Center* (VRTC) sobre los riesgos de ciberseguridad de la arquitectura de los vehículos, con el objetivo de establecer principios, reglas y requisitos para el diseño de vehículos en relación a la seguridad.

En resumen, la ciberseguridad en el ámbito automovilístico es algo que debe ajustarse a los rápidos avances tecnológicos de este sector y además de aportar una fiabilidad extra debido a que una vulnerabilidad puede impactar directamente en la seguridad física de los ocupantes del vehículo.

VULNERABILIDADES

Reciba nuestro boletín completo de parches y vulnerabilidades suscribiéndose [aquí](#).

Atlassian

CVE-2023-22501

Fecha: 03/02/2023

Descripción. El pasado 3 de febrero se publicó una vulnerabilidad de autenticación crítica que afecta a Jira Service Management Server and Data Center y que podría permitir a un atacante suplantar la identidad de un usuario y obtener acceso a una instancia de Jira. Para la explotación de la vulnerabilidad CVE-2023-22501 es necesario tener acceso de escritura a un directorio de usuarios y el correo electrónico saliente debe estar habilitado en la instancia de Jira Service Management. Con estas condiciones un atacante podría obtener acceso a los tokens de suscripción de usuarios con cuentas en las que nunca han iniciado sesión.

El acceso a los tokens podría ocurrir de dos formas:

- El atacante está incluido en las incidencias o solicitudes con los usuarios.
- El atacante es el return path del correo o puede obtener acceso a correos electrónicos de estos usuarios que contengan un enlace de "View Request".

Enlace: <https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/fallo-autenticacion-productos-jira-atlassian>
<https://jira.atlassian.com/browse/JSDSERVER-12312>

Productos afectados. Esta vulnerabilidad afecta a las siguientes versiones o anteriores de Jira Service Management Server and Data Center:

- 5.3.0; 5.3.1; 5.3.2; 5.4.0; 5.4.1 y 5.5.0

Solución: La solución principal para solventar esta vulnerabilidad consiste en actualizar Jira Service Management Server and Data Center a las siguientes versiones:

- 5.3.3; 5.4.2; 5.5.1, 5.6.0 o posterior

En caso de no poder actualizar de forma inmediata Jira Service Management se plantea como mitigación temporal actualizar el archivo JAR, que se puede encontrar en:

<https://confluence.atlassian.com/jira/jira-service-management-server-and-data-center-advisory-cve-2023-22501-1188786458.html>

OpenSSL

CVE-2023-0286

Fecha: 08/02/2023

Descripción. Múltiples vulnerabilidades asociadas al proyecto OpenSSL han sido detectadas, incluyendo una de severidad alta. Dicha vulnerabilidad podría permitir a los atacantes leer contenidos de la memoria y provocar ataques de denegación de servicio. Este fallo de seguridad se produce con una confusión de tipo al tratar las direcciones X.400 procesadas dentro de un GeneralName X.509. Es importante destacar que en la mayoría de casos, el ataque requiere que el atacante proporcione tanto la cadena del certificado así como la CRL, sin tener que estar firmadas ninguna de ellas necesariamente. Por lo tanto, es más probable que esta vulnerabilidad afecte únicamente a aplicaciones que hayan implementado de forma individual la recuperación de CRLs a través de la red.

Enlace: <https://thehackernews.com/2023/02/openssl-fixes-multiple-new-security.html>
<https://nvd.nist.gov/vuln/detail/CVE-2023-0286>

Productos afectados.

Versiones de OpenSSL comprendidas entre:

- Desde 3.0.0 y anteriores a 3.0.8
- Desde 1.1.1 y anteriores a 1.1.1t
- Desde 1.0.2 y anteriores a 1.0.2zg

Solución: Desde el fabricante se ha instado a actualizar los últimos parches publicados:

- 3.0.8
- 1.1.1t
- 1.0.2zg

PARCHES

Android

Fecha: 07-02-2023



Descripción. Android ha publicado su boletín mensual del mes de febrero, donde ha remediado una serie de vulnerabilidades de severidad crítica y alta. Dichas vulnerabilidades afectan al propio sistema operativo, así como a varios componentes y podrían permitir la escalada de privilegios, divulgación de información y la generación de ataques de denegación de servicio (DoS).

Las vulnerabilidades de seguridad crítica se detallan a continuación:

- Vulnerabilidad en el subcomponente kernel de Qualcomm.
- Vulnerabilidad en el subcomponente Bluetooth de Qualcomm.
- 2 vulnerabilidades en los subcomponentes closed-source de Qualcomm.

Enlace:

<https://www.incibe-cert.es/alerta-temprana/aviso-seguridad/boletin-seguridad-android-febrero-2023>

<https://source.android.com/security/bulletin?hl=es-419>

Productos afectados:

- Android Open Source Project (AOSP): versiones 10, 11, 12, 12L y 13.
- Componentes:
 - framework,
 - media framework,
 - system,
 - sistema de actualizaciones de Google Play,
 - kernel,
 - MediaTek,
 - Unisoc,
 - Qualcomm (incluidos closed-source).

Solución: Actualizar los parches de seguridad publicados por el fabricante de dispositivo correspondiente.

Cisco

Fecha: 02-02-2023



Descripción. Cisco ha publicado una serie de parches de seguridad para sus productos. Dichos parches corrigen una serie de vulnerabilidades de severidad alta y media. Estas vulnerabilidades podrían permitir a un atacante realizar las siguientes acciones:

- Tomar control remoto de los sistemas afectados
- Ejecutar comandos arbitrarios con permisos de root.
- Causar ataques de denegación de servicio (DoS).
- Llevar a cabo ataques de Cross-Site Scripting (XSS).

Enlace: <https://www.cisa.gov/uscert/ncas/current-activity/2023/02/02/cisco-releases-security-advisories-multiple-products>

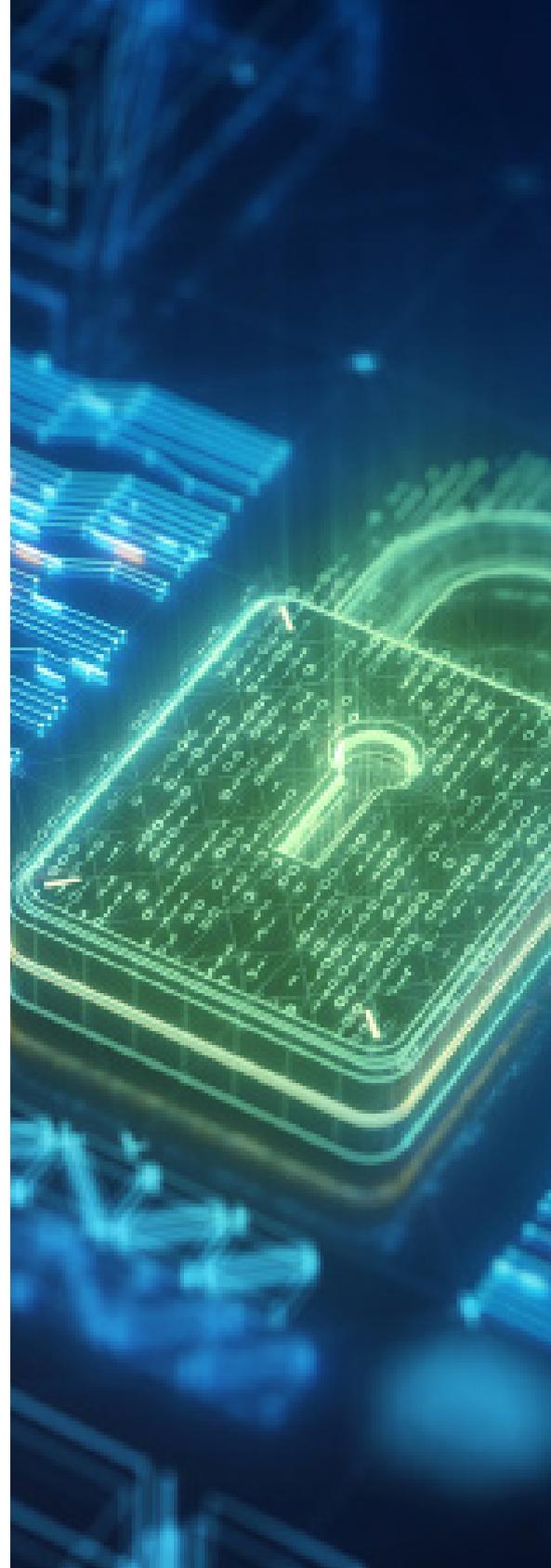
<https://sec.cloudapps.cisco.com/security/center/publicationListing.x>

Productos afectados:

Los productos afectados son los siguientes:

- Cisco IOx Application Hosting Environment
- Cisco BroadWorks Application Delivery Platform
- Xtended Services Platform
- Cisco Identity Services Engine

Solución: Actualizar a las nuevas versiones de los productos afectados.



EVENTOS

III edición de Alta Dirección, Concienciación e Implicación en Ciberseguridad

7 de marzo de 2023 |

El próximo 7 de marzo llega la III Edición de la Alta Dirección, Concienciación e Implicación en Ciberseguridad, evento organizado por la Fundación Borredá en colaboración con la revista Red Seguridad, donde altos directivos de empresas comparten en formato TV Experience su experiencia en cuanto a la implementación de la ciberseguridad en sus compañías, junto con su visión sobre el proceso de digitalización y cómo han hecho frente a la ciberguerra. A pesar de que todavía no se ha confirmado los detalles del lugar de encuentro, se espera que un gran número de personas interesadas en el mundo de ciberseguridad se unan a este evento, tomando como referencia que, en años anteriores, pudieron superar un foro de más de 500 personas.

Enlace: https://www.redseguridad.com/agenda/iii-jornada-de-alta-direccion-concienciacion-e-implicacion-con-la-ciberseguridad_20221230.html

RootedCon 2023

9 - 11 de marzo 2023 |

Del 9 al 11 de marzo se celebra la XVI edición del RootedCON 2023. Esta conferencia de ciberseguridad se trata un lugar de debate donde distintos profesionales comparten sus conocimientos sobre seguridad informática. Durante este evento también se celebran las RootedLab, donde se presentan diferentes actividades formativas para que los participantes puedan poner a prueba sus conocimientos de ciberseguridad; además de las Bootcamps, donde se habilita que especialistas profundicen en un tema avanzado durante dos días intensivos de formación. Esta conferencia es la mejor oportunidad para aquellos que quieran actualizar sus conocimientos prácticos y teóricos en el mundo de seguridad informática.

Enlace: <https://www.rootedcon.com/index/>

II Congreso Ciberseguridad de Andalucía

22 - 23 de marzo de 2023 |

La Junta de Andalucía y la Agencia Digital de Andalucía organiza del 22 al 23 de marzo el II Congreso de Ciberseguridad de Andalucía, que tendrá lugar en el Palacio de Ferias y Congresos de Málaga. Este congreso busca convertirse en un punto de encuentro primordial entre las agencias privadas, los profesionales y la administración pública, pudiendo de esta manera reforzar las capacidades de detección, prevención y respuesta ante incidentes que puedan afectar a la administración y organismos públicos. A pesar de que todavía no se haya confirmado la agenda concreta del evento ni los exponentes que intervendrán en la propuesta, actualmente se conoce que se contará con una serie de exposiciones profesionales de ciberseguridad, además de diferentes desafíos que todavía quedan por superar tras la inauguración de la edición anterior.

Enlace: <https://www.juntadeandalucia.es/congresociberseguridadandalucia/>

ASLAN Congress 2023

22 - 23 de marzo de 2023 |

En el Palacio de Congresos de Madrid tendrá lugar la 30ª Edición del Congreso Aslan 2023 desde el 22 al 23 de marzo. En este congreso, al igual que en ediciones anteriores, participarán más de 150 representantes y especialistas para abordar temas relacionados con las tendencias tecnológicas actuales, dividiéndose en 5 grandes bases: Data Management, Cloud Data Center, Intelligent Network, Digital Workspace y Ciberseguridad. Algunas de las actividades principales que se podrá encontrar en este congreso son: Forum de Ciberseguridad e Innovación digital, Digital Workspace, Ciberseguridad en las PYMES y Data Management & IA, entre muchos otros.

Enlace: <https://aslan.es/congreso2023/>



RECURSOS

XSS Hunter

XSS Hunter (nueva versión): Es una herramienta desarrollada por Truffle Security que permite identificar vulnerabilidades de cross-site scripting (XSS) en sitios Web. La nueva versión es un fork de la versión open source (<https://github.com/mandatoryprogrammer/xsshunter>) con nuevas características y seguridad mejorada.

Enlace: https://portswigger.net/daily-swig/truffle-security-relaunches-xss-hunter-tool-with-new-features?&web_view=true

GRR

Herramienta de Google para análisis forense remoto. Es un marco de respuesta a incidentes haciendo uso de análisis forense remoto en vivo. El objetivo de GRR es respaldar el análisis forense y las investigaciones de una manera rápida y escalable para permitir que los analistas clasifiquen rápidamente los ataques y realicen análisis de forma remota. GRR se creó para ejecutarse a escala, de modo que los analistas sean capaces de recopilar y procesar datos de manera efectiva de una gran cantidad de máquinas. <https://github.com/google/grr>

Enlace: <https://noticiasseguridad.com/tutoriales/como-usar-esa-herramienta-de-google-para-analisis-forense-remoto/>

WAFARAY

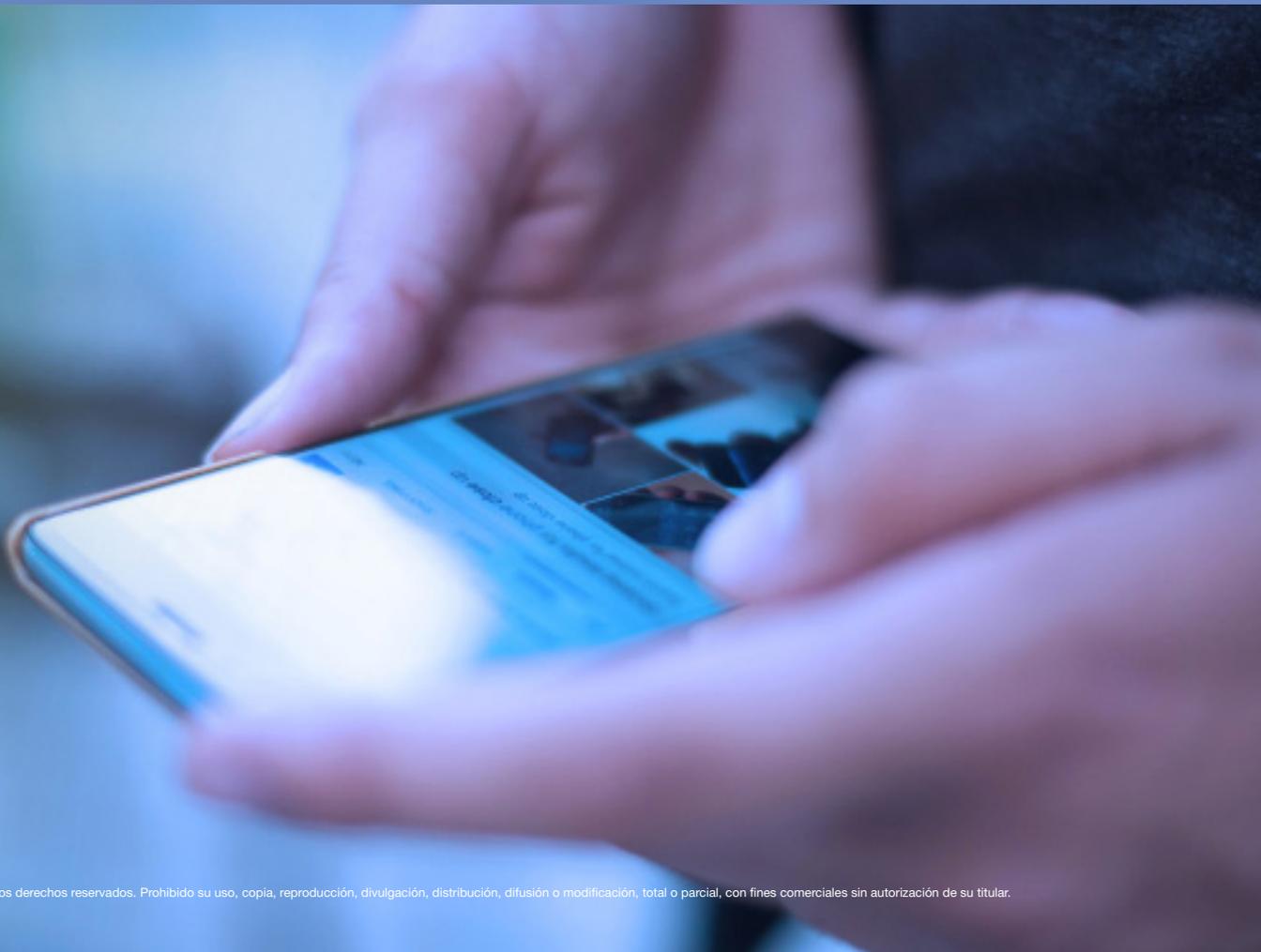
Herramienta que hace uso de WAF más YARA para detectar malware en el nivel WAF antes de que WAF pueda reenviarlos al backend, por ejemplo, archivos cargados a través de funciones web. Utiliza reglas YARA precompiladas y listas para usar a través de ModSecurity (WAF) usando una regla personalizada, que realizará una inspección y detección de los archivos que puedan contener código malicioso, típicamente funciones web (cargar archivos), y si el archivo es sospechoso los rechazará.

Enlace: <https://noticiasseguridad.com/tutoriales/wafaray-mejora-tu-deteccion-de-malware-con-waf-yara/>

OSV Scanner

Herramienta gratuita de Google para la identificación y evaluación de vulnerabilidades en dependencias de terceros mediante el uso de la base de datos OSV. Está disponible como una herramienta de línea de comandos y permite escanear un directorio de dependencias y generar un informe con cualquier vulnerabilidad que se encuentre. Se puede integrar en CI de GitLab. <https://github.com/google/osv-scanner>

Enlace: <https://www.cibertip.com/ciberseguridad/google-lanza-herramienta-gratis-osv-scanner-para-evaluacion-de-vulnerabilidades/>





NTT Data
Trusted Global Innovator

powered by the
cybersecurity **NTT DATA** team

nttdata.com