NÚMERO 82 | SEPTIEMBRE 2023

NTT DATA
Trusted Global Innovator

Radar

El magazine de ciberseguridad

SALVAGUARDANDO LA FRONTERA DIGITAL CON CIAM

La ciberseguridad y la protección de datos son las bases para generar confianza con los clientes, ya que salvaguardar sus datos es la prioridad número uno de cualquier empresa. Para ello las compañías se han centrado habitualmente en las soluciones de gestión de identidades y accesos (IAM) centradas en los usuarios internos de una organización. Sin embargo, la Gestión de Identidades y Accesos de Clientes o Customer Identity and Access Management (CIAM) esuna solución de vanguardia que permiten a las organizaciones gestionar de forma segura las identidades de sus clientes y el acceso a sus servicios. La CIAM atienda específicamente a los requisitos únicos de los clientes externos, socios y proveedores, garantizando una experiencia segura y fácil de usar.

Importancia en la Ciberseguridad Moderna

El CIAM ofrece robustos mecanismos de autenticación y autorización, mitigandoel riesgo de acceso no autorizado y fraude de identidad. Con el creciente número de brechas de datos y ciberataques, proteger las identidades de los clientes se ha convertido en una prioridad urgente para las empresas que buscan mantener una ventaja competitiva al tiempo que conservan la confianza de sus clientes.

Su papel también es fundamental tras la implementación de rigurosas regulaciones de protección de datos, como el Reglamento General de Protección de Datos (GDPR), ya que las empresas que manejan datos de clientes deben cumplir con estas normativas. El CIAM ofrece un enfoque integral para cumplir con los requisitos de cumplimiento, reduciendo la probabilidad de sanciones y daños a la reputación. Las soluciones de CIAM están diseñadas para manejar un gran número de identidades y transacciones de clientes simultáneamente. Esta capacidad de escalabilidad asegura que las organizaciones puedan gestionar de manera efectiva los requisitos de identidad y acceso, incluso durante períodos de uso máximo.

Todo esto se logra mediante una experiencia de usuario personalizada que permite a las empresas obtener valiosos conocimientos sobre el comportamiento y las preferencias de los clientes. Esta información puede utilizarse para ofrecer servicios y experiencias personalizadas, mejorando así la satisfacción y aumentando la lealtad del cliente.

Los oponentes clave

Desde procesos de registro simplificados hasta análisis avanzados de seguridad, veamos los elementos esenciales que hacen del CIAM un elemento transformador en el ámbito de la gestión de identidad digital.

1. **Registro e Integración:** Proceso de registro fluido. Los clientes deberían poder crear cuentas de forma fácil y segura, lo que les permitiría acceder a los servicios con una fricción mínima.
2. **Autenticación:** Empleo de diversos métodos de autenticación, como la autenticación multifactorial (MFA), la verificación biométrica y el inicio de sesión único (SSO). Estos mecanismos garantizan que solo los usuarios autorizados puedan acceder a los recursos que necesitan.
3. **Gestión de Consentimiento:** Funciones de gestión de consentimiento que otorgan a los clientes el control sobre sus datos personales y su uso. Esto se alinea con las regulaciones de privacidad de datos y refuerza la transparencia y la confianza.
4. **Gestión de Perfiles:** Permite a los clientes administrar sus perfiles y preferencias, como la actualización de información personal, preferencias de correo electrónico y configuraciones de comunicación.
5. **Análisis de Seguridad:** Análisis de seguridad para detectar actividades sospechosas y posibles amenazas, lo que permite a las organizaciones responder de manera proactiva a los riesgos de seguridad emergentes.

Los desafíos de implementación de CIAMLa implementación del CIAM, a pesar de sus numerosas ventajas, no está exenta de desafíos. Uno de los obstáculos clave es lograr un equilibrio entre implementar medidas de seguridad sólidas y proporcionar una experiencia fluida y amigable para el usuario. Si bien los protocolos de seguridad sólidos son esenciales para proteger los datos del cliente, crear procesos excesivamente complejos pueden disuadir a los usuarios y llevar al abandono de registros o transacciones. Manejar y almacenar los datos de los clientes de forma segura mientras se preserva la privacidad de los datos es otro desafío significativo para las organizaciones. Con las crecientes regulaciones de protección de datos, las soluciones CIAM deben garantizar un estricto cumplimiento y priorizar la protección del derecho a la privacidad del cliente.

Además, a medida que las empresas crecen y las bases de clientes se expanden, este sistema debe poder escalarse para satisfacer la creciente demanda de servicios de gestión de acceso e identidad. Asegurar un rendimiento óptimo durante períodos de alta actividad de usuarios es crucial para mantener una experiencia positiva para el cliente.

El camino a la vanguardia

El CIAM es un componente esencial de las estrategias de ciberseguridad modernas. Las organizaciones pueden construir y mantener la confianza del cliente, fomentar la lealtad a la marca y crear un entorno digital seguro y personalizado para sus clientes. A medida que las amenazas cibernéticas continúan evolucionando, el CIAM puede ser un aliado poderoso para proteger la frontera digital y fortalecer la relación entre el cliente y el negocio.

Enrique Bernao Rosado
Manager de Ciberseguridad en NTT DATA Europe & Latam

CIBERCRÓNICA

Comenzamos esta nueva edición del RADAR con la siguiente noticia. Microsoft ha dado la voz de alarma tras descubrir que un conocido grupo de hackers vinculado al gobierno ruso ha estado utilizando la aplicación de chat Microsoft Teams para realizar ataques de phishing en organizaciones específicas.

El grupo, conocido como "Midnight Blizzard", ha sido identificado como una amenaza vinculada al Servicio de Inteligencia Exterior de la Federación de Rusia (SVR). Utilizando Microsoft Teams, los hackers han llevado a cabo una campaña de phishing dirigida contra objetivos en sectores gubernamentales, organizaciones no gubernamentales (ONG), servicios de tecnología, fabricación y medios de comunicación.
El modus operandi de Midnight Blizzard implica el uso de tenants de Microsoft 365 previamente comprometidos, propiedad de pequeñas empresas, para crear nuevos dominios que se hacen pasar por entidades de soporte técnico legítimas. A través de mensajes en Microsoft Teams, los hackers intentan robar credenciales de las organizaciones objetivo, solicitando a los usuarios la aprobación de autenticaciones multifactor (MFA).

> "Es fundamental estar alerta ante tácticas de phishing y reforzar las defensas en línea para protegerse contra estos sofisticados ataques. La colaboración y la vigilancia constante son esenciales en la lucha contra las crecientes amenazas cibernéticas."

Los ataques altamente selectivos han afectado a menos de 40 organizaciones únicas en todo el mundo, lo que sugiere una operación de ciberespionaje muy enfocada en objetivos en Estados Unidos y Europa.

Una vez que los usuarios aceptan los mensajes y siguen las instrucciones, los hackers obtienen credenciales válidas para acceder a las cuentas de Microsoft 365 de las víctimas. Posteriormente, se han detectado actividades de robo de información en los tenants comprometidos. Además, en algunos casos, los hackers intentan agregar dispositivos a las organizaciones como dispositivos administrados para eludir políticas de acceso condicional.

Microsoft ha tomado medidas para mitigar el uso de los dominios por parte de este grupo, y continúa investigando otros ataques relacionados. Este incidente destaca la importancia de la concienciación y la seguridad cibernética en las organizaciones. Es fundamental estar alerta ante tácticas de phishing y reforzar las defensas en línea para protegerse contra estos sofisticados ataques. La colaboración y la vigilancia constante son esenciales en la lucha contra las crecientes amenazas cibernéticas.

Por otro lado, surge una nueva herramienta de inteligencia artificial (IA) llamada "FraudGPT", dirigida específicamente a ataques sofisticados. Los actores malintencionados la están promocionando en mercados de la dark web y canales de Telegram. Diseñada para fines ofensivos, la herramienta permite crear correos electrónicos de spear phishing, desarrollar malware indetectable, encontrar vulnerabilidades y más... Su autor afirma que ha habido más de 3,000 ventas y revisiones confirmadas.

La herramienta ha estado circulando desde al menos julio de 2023 y se ofrece a través de un modelo de

suscripción con un costo de 200$ al mes, 1.000$ por seis meses y 1.700$ por un año. Aunque el modelo de lenguaje específico utilizado para desarrollar FraudGPT aún se desconoce, esta nueva generación de herramientas de IA para ciberdelincuentes plantea desafíos significativos para la ciberseguridad.

Estas herramientas pueden actuar como un lanzamiento para script kiddies que buscan llevar a cabo ataques de phishing empresariales a gran escala, lo que podría resultar en el robo de información confidencial y pagos no autorizados. Frente a este escenario, se vuelve esencial implementar estrategias de defensa en profundidad y contar con una rápida telemetría de seguridad para detectar y contrarrestar amenazas antes de que se conviertan en incidentes de mayor gravedad.

También cabe destacar la siguiente noticia. El número de ataques de ransomware a organizaciones industriales e infraestructura se ha duplicado desde el segundo trimestre de 2022, según un informe de Dragos, una firma de ciberseguridad industrial. En el segundo trimestre de 2023, se registraron 253 incidentes, lo que representa un aumento del 18% respecto al primer trimestre del mismo año, donde se observaron 214 ataques. La compañía atribuye el aumento de ataques a una disminución de los ingresos por ransomware en 2022, ya que más víctimas se niegan a pagar. Además, se espera que los ataques continúen aumentando debido a las tensiones políticas entre los países de la OTAN y Rusia, lo que motiva a los grupos de ransomware asociados con Rusia a seguir atacando infraestructuras críticas en países de la OTAN. También se ha observado que los grupos de ransomware se enfocan en atacar a organizaciones más grandes para mantener sus ingresos. El sector de manufactura es el más afectado, seguido de los sistemas de control industrial (ICS), transporte y petróleo y gas.

Uno de los ataques más polémicos de este mes ha sido el que ha tenido como víctima a CardioComm, proveedor canadiense de soluciones médicas de monitoreo cardíaco, ha sido víctima de un ciberataque que ha obligado a la compañía a suspender sus operaciones. Los servidores de producción se vieron afectados, lo que llevó a la interrupción de los servicios en su sitio web. La empresa estima que su negocio se verá impactado durante varios días, mientras trabaja para restaurar los datos y los entornos de servidores.

Aunque el ataque no comprometió la información de salud de los clientes, CardioComm ha tomado precauciones para proteger la información personal de sus empleados. Se sospecha que el ataque podría haber sido perpetrado por ransomware, lo que llevó a la empresa a tomar medidas inmediatas para contener la situación y evitar mayores daños.

Además, el ciberataque podría tener consecuencias financieras, ya que CardioComm podría enfrentar dificultades para finalizar presentaciones requeridas debido a una orden de cese de operaciones emitida por la Comisión de Valores de Ontario, lo que también resultó en la suspensión de la negociación de sus acciones.

CardioComm es conocido por proporcionar software especializado para grabar y analizar electrocardiogramas, utilizado por hospitales, médicos y dispositivos de consumo para el diagnóstico de pacientes con problemas cardíacos. La compañía trabaja arduamente para superar esta situación y restaurar la normalidad en sus operaciones.

¿PODEMOS CONFIARLE NUESTRA PRIVACIDAD A CHATGPT?

Por: NTT DATA Europe & Latam

Si ustedes no viven en otro planeta, sabrán lo que es ChatGPT. La parte de "Chat" queda más o menos clara solo con el primer uso, sin embargo, las siglas GPT esconden mucho más de lo que se puede apreciar a simple vista.

Generative, Pre-trained & Transformer. ChatGPT es un modelo de Inteligencia Artificial (en adelante IA) que se basa en la tecnología OpenAI para crear nuevo contenido (texto o diálogo) y que se entrena usando una gran colección que gracias a una red neuronal que aprende y mejora de manera constante. Se limita a replicar el modo en que los humanos hablamos, aprende sobre la base de muchos textos, pero se queda en la capa superficial de la semántica y de la sintáctica. Tampoco verifica la fiabilidad de la información y con toda la desinformación que nos rodea eso puede ser peligroso. Del mismo modo que no reconoce el sarcasmo o el sentido del humor.

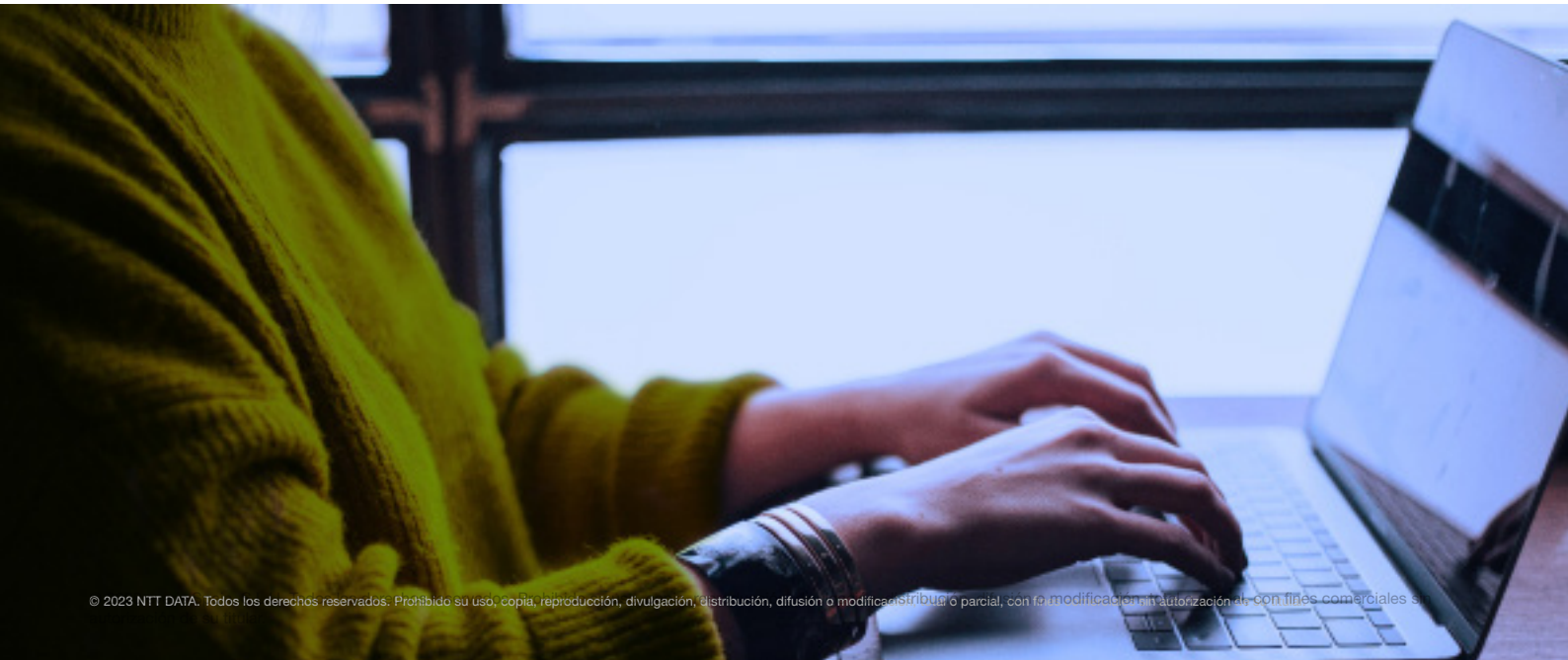
La IA no funciona sola, necesita un "copiloto", las personas. ¿Por qué una máquina necesita tener detrás a un humano? Por las garantías. No podemos negar que estamos en el ojo de una tormenta perfecta entre la tecnología y la innovación, ya que tenemos a nuestra disposición los medios necesarios para ejecutar herramientas como ChatGPT, y, además se están dando las condiciones ideales para que esos procesos sean eficientes y que las decisiones de la IA tengan relevancia e impliquen una adecuada protección de datos.

Las intersecciones entre la inteligencia artificial y la normativa de protección de datos son evidentes. Un ejemplo de esto es su política de privacidad, que no aclara cómo trata y protege los datos personales para generar contenido.

Lo que sí está claro es que los usa. El chat se alimenta de una cantidad masiva de textos recogidos en internet (blogs, artículos, foros públicos, páginas web…) por lo que, si nuestros datos se encuentran en alguno de los sitios mencionados: ChatGPT tiene acceso a ellos.

Por no hablar de todo lo que aprende de nuestros matices, la forma en la que preguntamos a la hora de conversar con él ¿nos está analizando? ¿está generando un perfil sin nuestro consentimiento? ¿es transparente con los usuarios?

Por eso la protección de datos es especialmente relevante con este tipo de sistemas basados en aprendizaje y no debemos olvidar las bases para que sean aplicaciones seguras para el usuario.



Hay 4 pilares esenciales en función de la normativa de protección de datos:

- Derechos en favor de los titulares de los datos.
- Principios del tratamiento de datos (las reglas de juego).
- Medidas de responsabilidad proactiva (basadas en el enfoque del riesgo).
- Autoridades de control.

La solución más evidente es establecer el sistema de privacidad desde el diseño. Actuando como un elemento bisagra entre la fase de diseño del sistema de inteligencia artificial y la fase de despliegue. Al final, el elemento clave es cómo conferimos el sistema de IA. En muchos casos si desde el diseño no ejecutamos el sistema adecuadamente para que cumpla posteriormente con la normativa de Protección de Datos, una vez que esta adopte decisiones, no se puede hacer nada. Cuando el sistema ya esté en el mercado, si no se ha implementado el elemento de privacidad desde la fase de diseño, posiblemente ese sistema de IA no cumplirá adecuadamente con la normativa de Protección de Datos.

¿Qué se quiere decir con fase de diseño y fase de despliegue? Veámoslo.

FASE DE DISEÑO DEL SISTEMA

- Fijación del Proyecto
- Recopilación de datos
- Elección de algoritmos
- Desarrollo de modelos
- Entrenamiento de modelos
- Evaluación de los modelos

FASE DE DESPLIGUE DEL SISTEMA

- Diferente organización (desarrolla/implementa)
- Integración en el entorno
- Inferencias realizadas del modelo
- Adopción de decisiones
- Monitorización del modelo

Lo primero que se hace cuando se inicia un proyecto es fijar el alcance, las 5W (what, who, where, why, when), tener claro el roadmap. Para que una IA funcione como queremos necesita de una gran cantidad de datos para que ésta pueda aprender. Una vez tenemos este coctel bajo control, desarrollamos, entrenamos y evaluamos los modelos generados.

Parece sencillo, pero aquí entra en juego uno de los cuatro pilares de la protección de datos, y es que si nos paramos detenidamente a analizar estas 3 palabras “recopilación de datos” entran en conflicto muchos de los principios de protección de datos.

Vamos a poner un ejemplo para que se vea más claro. Ponemos a la IA en funcionamiento y la alimentamos con datos masivos, indiscutiblemente el principio de minimización de datos se va a ver afectado. Pero claro, necesitamos que multitud de bases de datos entren en juego para que los datos estén lo más actualizados posibles y que las variables sean lo suficientemente representativas. Si ésta genera inferencias, los datos podrías ser inexactos y no queremos que eso pase… principio de exactitud.

¿Cómo ejecutar correctamente programas implementando el *Privacy by Design* desde el punto de vista del DPD? Está claro que soluciones de este tipo deben ser diseñadas cumpliendo desde el principio con el marco normativo, ¿cómo? Con una justificación adecuada de variables elegidas por las fases del proceso, estableciendo las finalidades del tratamiento, a donde se quiere llegar, analizar la compatibilidad entre el fin inicial y el fin último… para cuando en la fase de despliegue del proyecto diferentes equipos entren en el ring, desarrolladores, QA, integradores… se muevan dentro de esos márgenes preestablecidos y poder cumplir con la normativa.

TENDENCIAS

La identidad autogobernada: el nuevo modelo de gestión de la identidad en ciberseguridad

La identidad autogobernada – en inglés *Self-Sovereign Identity* (SSI) – es un modelo de gestión de la identidad digital que evita quela autenticación recaiga en una única autoridad central y soberana. En contraste con los modelos tradicionales donde los gobiernos y las compañías son los custodios de nuestros datos, un sistema de identidad autogobernada se basa en la capacidad del individuo para administrar y compartir su información de manera segura y selectiva. Es decir, se intercambian los roles poniendo el foco en modelos donde el usuario decida qué pueden ver sobre nosotros y qué no.

Para conseguir una autogestión de la identidad, tendremos que basarnos en el uso de estostres pilares básicos:

- **Blockchain:** registro de la información de manera digital y descentralizada, utilizando la criptografía dentro de una cadena de bloques en la que, debido a su forma de estructurarse impedirá que ésta sea modificable por terceros con éxito.
- **Identificadores descentralizados (DIDs):** código único para cada individuo que permite una identificación única del mismo, así como gestionar a qué información se quiere dar acceso desde el wallet (aplicación o dispositivo que permite almacenar y gestionar criptomonedas y activos digitales), en el cual se recoge la misma para identificarse. Para ello se realiza una conexión segura entre dos partes usando un par de claves públicas y una o varias claves privadas.
- **Credenciales verificables (VCs):** las identidades se encuentran encriptadas y securizadas para así poder ser verificadas por cualquier organismo de manera rápida y eficiente, sin tener que consultar directamente sus datos personales.

El uso del wallet, mencionado anteriormente, permite en estos modelos SSI que la gestión de la información compartida por el individuo recaiga en él al completo. Además, permite realizar esta acción dónde y cuándo sea,usando un único identificador para ello. Esto impedirá a su vez que su identidad desaparezca si es eliminada por el organismo que la gestiona o si no es válida en otro contexto que no sea el que recoge la entidad responsable.

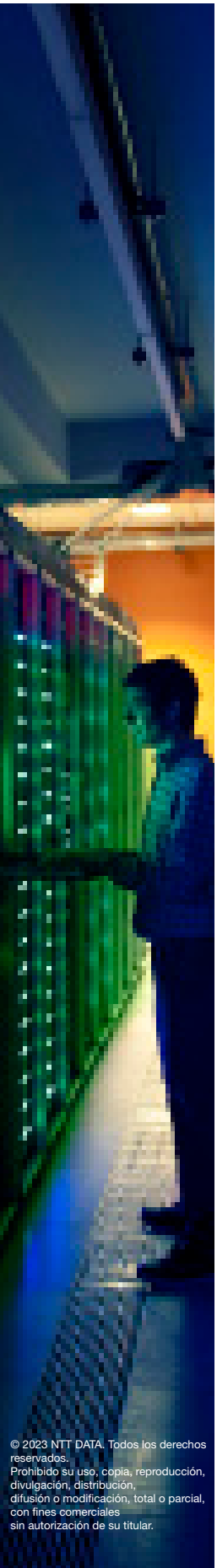
Dentro de este planteamiento encontramos el concepto que se conoce como “triángulo de confianza”, compuesto por: holder (usuario que genera el identificador descentralizado en el wallet), issuer (autoridad que emite las credenciales verificables) y verifier (parte encargada de verificar la credencial).

Un ejemplo de uso sería la solicitud de plaza en un grado universitario, donde se solicita al estudiante (holder) mostrar su identificador en el wallet para comprobar que posee el título de bachillerato requerido (cuyo issuer sería una institución educativa). Al compartir esta información, se establece una conexión segura entre la universidad y el usuario. Solo se revela la información necesaria, manteniendo la privacidad de otros datos personales, que no han sido revelados debido a que el usuario selecciona qué es lo que puede consultarse. La universidad (verifier) verifica la autenticidad de los datos usando la identidad digital y la clave pública asociada almacenadas en el blockchain.

Este enfoque de gestión de identidad es más seguro y eficiente que los métodos tradicionales, al evitar la centralización y los riesgos de robo de credenciales. El usuario tiene el poder de decidir quién accede a su información, reduciendo el riesgo de escalada de privilegios y el seguimiento no autorizado. En conjunto, la Identidad Autogobernada y las Credenciales Verificables representan un avance significativo en la protección de la identidad digital y la privacidad en un entorno cada vez más digitalizado.

VULNERABILIDADES

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



Citrix

CVE-2023-3519;-3466;-3467
Fecha: 18/07/2023

Descripción.Se han publicado tres vulnerabilidades que afectan a productos de Citrix (NetScaler ADC y Citrix Gateway). Una de ellas es de severidad crítica (CVE-2023-3519) y las otras dos de severidad alta (CVE-2023-3466 y CVE-3467). La vulnerabilidad crítica (CVE-2023-3519) aprovecha un error que permite la inyección de código y, por lo tanto, la ejecución remota de código por parte de los atacantes. Para poder explotar esta vulnerabilidad es necesario que el dispositivo esté configurado como Gateway. Una de las vulnerabilidades altas (CVE-2023-3466) consiste en la posibilidad de ejecutar ataques Cross-Site Scripting debido a la falta de validación de los datos de entrada. La explotación exitosa de esta vulnerabilidad requiere que el atacante envíe una URL a la víctima. La última vulnerabilidad alta (CVE-2023-3467) aprovecha una inadecuada gestión de privilegios, de forma que se permite escalar privilegios dentro del producto vulnerable.

Enlace: https://www.ccn-cert.cni.es/seguridad-al-dia/avisos-ccn-cert/12672-ccn-cert-av-08-23-actualizacion-de-seguridad-en-productos-citrix.html
https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467

Productos afectados. Los productos afectados son los siguientes:

- NetScaler ADC y NetScaler Gateway 13.1 antes de 13.1-49.13
- NetScaler ADC y NetScaler Gateway 13.0 antes de 13.0-91.13
- NetScaler ADC 13.1-FIPS antes de 13.1-37.159
- NetScaler ADC 12.1-FIPS antes de 12.1-55.297
- NetScaler ADC 12.1-NDcPP antes de 12.1-55.297

Solución: La solución propuesta por el fabricante consiste en actualizar a las siguientes versiones:

- NetScaler ADC y NetScaler Gateway 13.1-49.13 y versiones posteriores
- NetScaler ADC y NetScaler Gateway 13.0-91.13 y versiones posteriores de 13.0
- NetScaler ADC 13.1-FIPS 13.1-37.159 y versiones posteriores de 13.1-FIPS
- NetScaler ADC 12.1-FIPS 12.1-55.297 y versiones posteriores de 12.1-FIPS
- NetScaler ADC 12.1-NDcPP 12.1-55.297 y versiones posteriores de 12.1-NDcPP

Ivanti EPM

CVE-2023-35082
Fecha: 03/08/2023

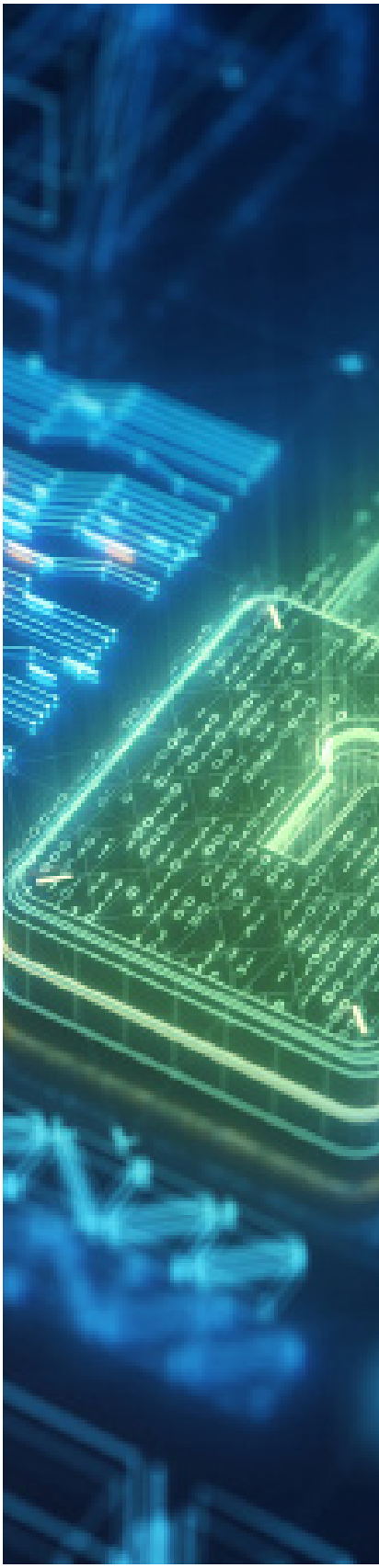
Descripción. El pasado mes de julio, se publicaron una serie de vulnerabilidades relativas a Ivanti EPMM. Dichas vulnerabilidades fueron corregidas con una serie de parches de seguridad. Sin embargo, un grupo de investigadores de ciberseguridad ha descubierto una forma de omitir las medidas de seguridad aplicadas por el fabricante, quedando dichas vulnerabilidades de nuevo al descubierto. La nueva vulnerabilidad de severidad crítica (CVE-2023-35082) surge del mismo lugar que la anterior (CVE-2023-35078) y podría permitir a un atacante acceder potencialmente a la información de identificación personal de los usuarios y realizar cambios limitados en el servidor. En concreto, un atacante con acceso a diferentes rutas de la API podría acceder a información de identificación personal (PII), como nombres, números de teléfono y otros detalles de dispositivos móviles para los usuarios en un sistema vulnerable.

Enlace: https://thehackernews.com/2023/08/researchers-discover-bypass-for.html
https://www.bleepingcomputer.com/news/security/ivanti-discloses-new-critical-auth-bypass-bug-in-mobileiron-core/

Productos afectados. La vulnerabilidad afecta a todas las versiones soportadas (11.4, 11.10, 11.9, 11.8 y anteriores).

Solución: Actualmente se está a la espera de que el fabricante publique nuevos parches que corrijan de forma definitiva estas vulnerabilidades.

PARCHES



Oracle

Fecha: 19-07-2023

Descripción. Oracle ha publicado una serie de actualizaciones para corregir 508 vulnerabilidades, incluyendo un total de 76 actualizaciones críticas y 183 CVEs únicos. Algunos de los productos con más parches y vulnerabilidades críticas se indican a continuación: El producto Oracle Construction and Engineering tiene un total de 147 parches y, además, 115 exploits remotos sin autenticación. Algunos de los CVEs para los que aplican los parches de este producto son: CVE-2023-1370, CVE-2023-24998 y CVE-2022-48285 entre otros. El producto Oracle Fusion Middleware tiene 60 nuevos parches de seguridad y 40 de esas vulnerabilidades se pueden explotar de forma remota sin autenticación. Algunos de los CVEs relacionados son: CVE-2022-42920, CVE-2022-45047, CVE-2023-25690, CVE-2021-42575 y CVE-2022-41853. El producto Oracle MySQL ha recibido 24 nuevas actualizaciones de seguridad. Sobre esas vulnerabilidades, 11 de ellas pueden ser explotadas de forma remota sin autenticación. El CVE con mayor criticidad que se ha solventado con las actualizaciones de seguridad es CVE-2023-20862.

Enlace:
https://www.ccn-cert.cni.es/component/vulnerabilidades/view/34497.html
https://www.oracle.com/security-alerts/cpujul2023.html

Productos afectados:
En total hay 32 productos diferentes de Oracle afectados.

Solución:
Aplicar los parches recomendados por Oracle en función del producto afectados.

Atlassian

Fecha: 18-07-2023

Descripción. Atlassian ha publicado varios parches de seguridad para sus productos. Dichos parches corrigen tres vulnerabilidades de severidad alta. Estas vulnerabilidades podrían permitir a un atacante realizar las siguientes acciones: Ejecución de código de forma remota. Esta vulnerabilidad permite a un atacante autenticado ejecutar código arbitrario con un alto impacto en la confidencialidad, alto impacto en la integridad, alto impacto en la disponibilidad y sin interacción del usuario (CVE-2023-22505). Ejecución remota de código que permite a un atacante autenticado ejecutar código arbitrario con un alto impacto en la confidencialidad, un alto impacto en la integridad, un alto impacto en la disponibilidad y sin interacción del usuario (CVE-2023-22508). Inyección y ejecución de código remoto permite a un atacante autenticado modificar las acciones realizadas por una llamada al sistema y ejecutar código arbitrario que tiene un alto impacto en la confidencialidad, un alto impacto en la integridad, un alto impacto en la disponibilidad y ninguna interacción con el usuario (CVE-2023-22506).

Enlace: https://www.cisa.gov/news-events/alerts/2023/07/21/atlassian-releases-security-updates
https://confluence.atlassian.com/security/security-bulletin-july-18-2023-1251417643.html

Productos afectados: Algunos de los productos afectados son los siguientes:
- Confluence Data Center & Server.
- Bamboo.

Solución: Aplicar los parches y actualizaciones publicados en el portal oficial del fabricante para cada uno de los productos afectados.

EVENTOS

Ciberseguridad sector salud

19 de septiembre de 2023 |

Evento de seguridad que se celebrará en Madrid tanto de forma presencial como virtual, con el objetivo de entrelazar los campos de conocimiento de la salud y la ciberseguridad, con el fin de estrechar la colaboración de todas las figuras involucradas en la protección de la información en el ámbito de la salud. Durante el congreso, se tratarán distintos retos que la digitalización de la salud traerá consigo desde el punto de vista de la ciberseguridad, como la aplicación de regulaciones, la problemática de los dispositivos médicos con conexión remota y el fortalecimiento de la resiliencia en el sector.

Enlace: https://ciberseguridadtips.com/congreso-de-ciberseguridad-en-el-sector-salud/

Cyber Security and Cloud Expo

26 - 27 de septiembre de 2023 |

Evento que tendrá lugar los dias 26 y 27 de septiembre en Ámsterdam que contará con conferencias de CISOs y discusiones sobre actualidad de ciberseguridad en entornos cloud, gestión de riesgos, ciber resiliencia, privacidad y normativa, gestión de la identidad, entre otros temas.

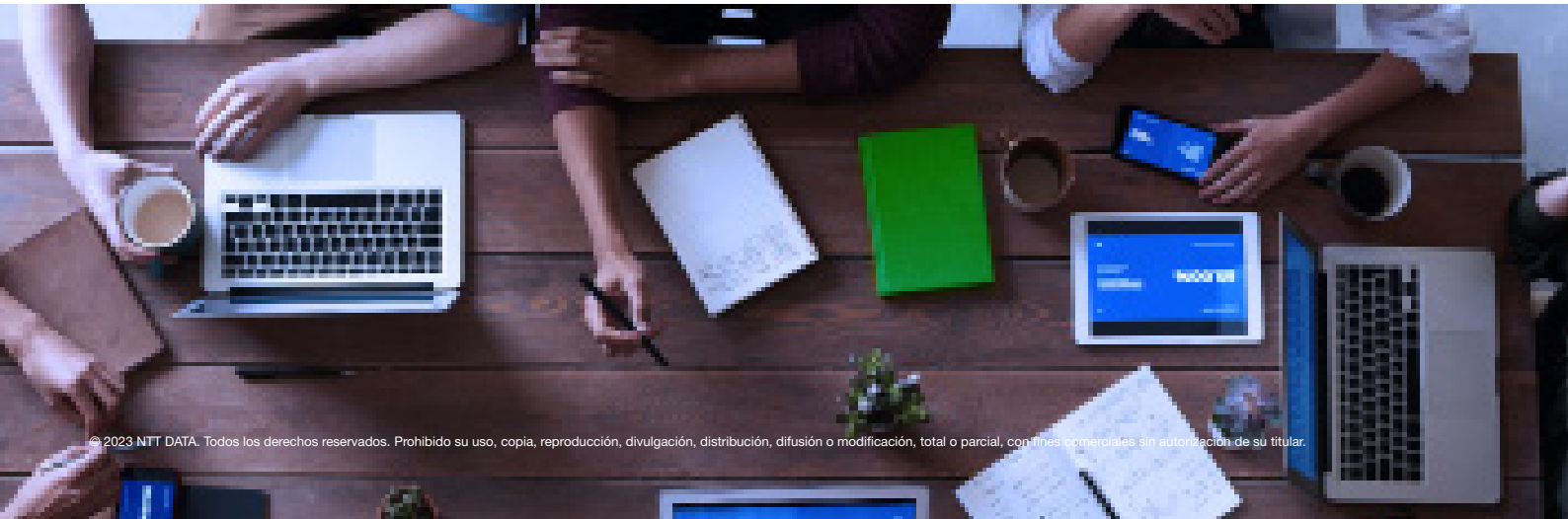
Enlace: https://cybersecuritycloudexpo.com/europe/

Gartner Security & Risk Management Summit

6 de julio 2023 |

Cumbre de Gartner que se celebrará en Londres, centrada en la gestión de riesgos para profesionales de la seguridad, donde se tratarán las posibilidades de fortalecimiento en ciberseguridad al alinearla con las estrategias de negocio de las compañías, generando un entorno más flexible y dinámico que mejore las capacidades de seguridad en los entornos digitales.

Enlace: https://www.gartner.com/en/conferences/emea/security-risk-management-uk



RECURSOS

Informe anual de vulnerabilidades 0-day en Android - Google

Google ha publicado el informe anual con el resumen de las vulnerabilidades 0-day detectadas en Android que han sido utilizadas por actores maliciosos. Desde que se comenzaron a publicar estos informes en 2014, este año ha sido el segundo con más vulnerabilidades 0-day detectadas. Entre otras conclusiones, se destaca como al no tener los fabricantes listos los parches de seguridad a tiempo, vulnerabilidades que cuentan con una remediación han podido ser utilizadas como vulnerabilidades 0-day contra los usuarios, al no poder contar en sus dispositivos con las actualizaciones necesarias.

Enlace: https://security.googleblog.com/2023/07/the-ups-and-downs-of-0-days-year-in.html

BlackLotus

BlackLotus se trata de un Bootkit UEFI diseñado específicamente para Windows, que tiene como propósito funcionar como un cargador HTTP. Esta herramienta incorpora un bypass de arranque seguro integrado, además de protección Ring0/Kernel para protegerse de cualquier intento de eliminación una vez se encuentre desplegado. Este software consiste de dos componentes principales: un Agente, que se instala en el dispositivo destino, y una Interfaz Web, utilizada por los administradores para gestionar los dispositivos con agente instalado. A pesar de que este ataque apareciese en fórums el año pasado, este mes se ha publicado su código fuente y ahora se encuentra accesible para cualquier usuario.

Enlace: https://github.com/ldpreload/BlackLotus

LetsCall

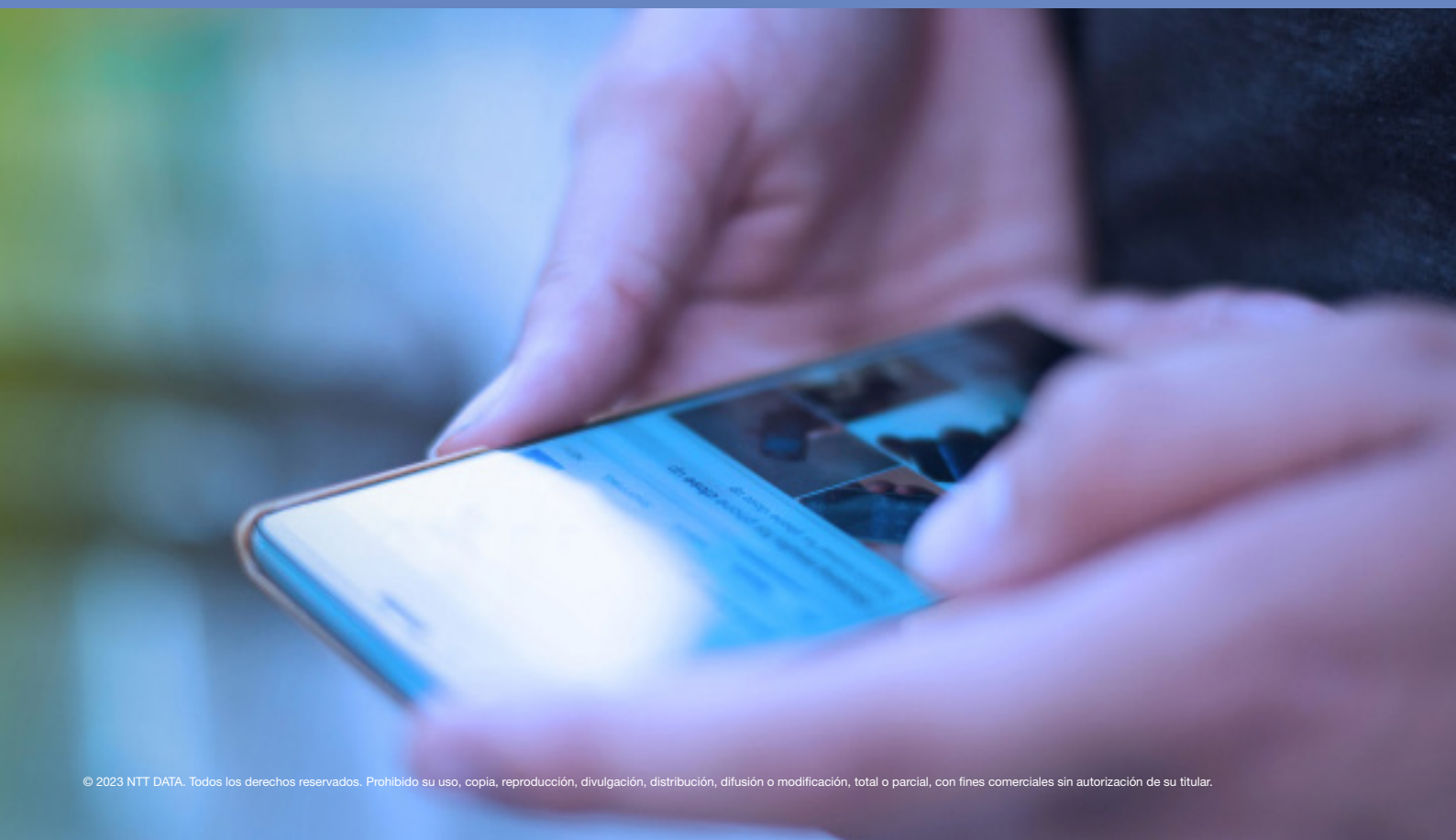
LetsCall es un nuevo conjunto de herramientas presenta un marco de trabajo fácil de usar a la hora de desarrollar y ejecutar ataques Vishing (Voice over IP Phising). Esto se debe a que presenta todas las instrucciones y herramientas donde no solo se describe cómo operar los dispositivos afectados, sino además cómo comunicarse con las posibles víctimas. Este marco de trabajo ya ha sido utilizado en lugares como Corea del Sur, donde se ha manifestado este ataque en el desarrollo del robo de un banco.

Enlace:https://www.threatfabric.com/blogs/letscall-new-sophisticated-vishing-toolset

WormGPT

Ha surgido una nueva herramienta denominada FraudGPT, que actualmente solo se proporciona a través de Telegram y se trata de la sucesora de la ya disponible WormGPT. Tanto FraudGPT como WormGPT proporciona un servicio de inteligencia artificial para diseñar y desarrollar maligno. Proporciona el mismo servicio que ChatGPT pero orientado a la creación de malware, proporcionando un servicio sin restricciones ni limitaciones éticas. Aunque el nuevo servicio de FraudGPT todavía no se encuentre disponible, ya es posible realizar la compra de la herramienta predecesora WormGPT.

Enlace: https://wormgpt.co/




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