NUMERO 82 | SEPTIEMBRE 2023

NTT DATA
Trusted Global Innovator

Radar

A revista da cibersegurança

PROTEGENDO A FRONTEIRA DIGITAL COM O CIAM

A cibersegurança e a proteção de dados são a base para conquistar a confiança dos clientes, já que a proteção de seus dados é a prioridade número um para qualquer empresa. Para isso, as empresas normalmente se concentram em soluções de gerenciamento de identidade e acesso (IAM, na sigla em inglês) voltadas para os usuários internos de uma organização. No entanto, o gerenciamento de acesso e identidade do consumidor (CIAM - Customer Identity and Access Management) é uma solução mais avançada que permite que as organizações gerenciem com segurança as identidades de seus clientes e o acesso a seus serviços. O CIAM trata especificamente dos requisitos exclusivos de clientes externos, parceiros e fornecedores, garantindo uma experiência segura e fácil de usar.

A importância do CIAM na cibersegurança moderna

O CIAM oferece mecanismos robustos de autenticação e autorização, mitigando o risco de acesso não autorizado e fraude de identidade. Com o crescente número de violações de dados e ciberataques, a proteção de identidades de clientes tornou-se uma prioridade urgente para as empresas que buscam manter uma vantagem competitiva e, ao mesmo tempo, preservar a confiança de seus clientes.

Sua função também é fundamental após a implementação de normas rigorosas de proteção de dados, como o Regulamento Geral sobre a Proteção de Dados (RGPD), pois as empresas que manipulam dados de clientes devem estar em conformidade com esses regulamentos. O CIAM oferece uma abordagem abrangente para atender aos requisitos de conformidade, reduzindo a probabilidade de penalidades e danos à reputação.

As soluções CIAM são projetadas para processar um número grande de identidades e transações de clientes simultaneamente. Essa escalabilidade garante que as organizações possam gerenciar com eficiência os requisitos de identidade e acesso, mesmo durante os períodos de pico de uso.

Tudo isso é obtido por meio de uma experiência de usuário personalizada que permite às empresas obter informações valiosas sobre o comportamento e as preferências dos clientes. Essas informações podem ser usadas para oferecer serviços e experiências personalizados, melhorando a satisfação e aumentando a fidelidade do cliente.

Principais desafios

De processos de registro simplificados a análises de segurança avançadas, vamos analisar os elementos essenciais que fazem do CIAM um componente transformador na área de gerenciamento de identidade digital.

- **Registro e integração:** Processo de registro eficiente. Os clientes devem ser capazes de criar contas com facilidade e segurança, permitindo que acessem serviços com menos dificuldade.
- **Autenticação:** Uso de diversos métodos de autenticação, como a autenticação multifator (MFA, na sigla em inglês), a verificação biométrica e o logon único (SSO, na sigla em inglês). Esses mecanismos garantem que somente usuários autorizados acessem os recursos de que precisam.
- **Gestão de consentimento:** Funções de gestão de consentimento permitem que os clientes tenham controle sobre seus dados pessoais e sua utilização. Isso está em conformidade com as normas de privacidade de dados e reforça a transparência e a confiança.
- **Gerenciamento de perfil:** Permite que os clientes gerenciem seus perfis e preferências, como a atualização de informações pessoais, preferências de e-mail e configurações de comunicação.
- **Análise de segurança:** Permite detectar atividades suspeitas e possíveis ameaças, possibilitando que as organizações respondam proativamente aos riscos de segurança emergentes.

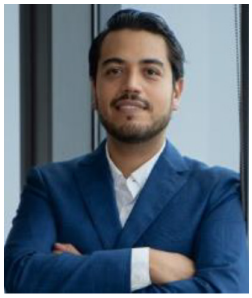
A implementação do CIAM, apesar de suas inúmeras vantagens, tem seus desafios. Um dos principais obstáculos é encontrar um equilíbrio entre a implementação de medidas de segurança sólidas e a oferta de uma experiência perfeita e de fácil utilização. Embora seja essencial ter protocolos de segurança robustos para proteger os dados dos clientes, a criação de processos excessivamente complexos pode desencorajar os usuários e levar ao abandono de registros ou transações.

Gerenciar e armazenar os dados dos clientes de forma segura e, ao mesmo tempo, preservar a privacidade dos dados é outro importante desafio para as organizações. Com o aumento das normas de proteção de dados, as soluções CIAM devem garantir uma conformidade rigorosa e priorizar a proteção à privacidade do cliente.

Além disso, à medida que as empresas crescem e as bases de clientes aumentam, esse sistema deve ter capacidade de escalonamento para atender à crescente demanda por serviços de gerenciamento de identidade e acesso. Garantir um desempenho otimizado durante os picos de atividade do usuário é fundamental para manter uma experiência positiva para o cliente.

O caminho para avançar

O CIAM é um componente essencial das estratégias modernas de cibersegurança. As organizações podem construir e manter a confiança do cliente, promover a fidelidade à marca e criar um ambiente digital seguro e personalizado para seus clientes. Conforme as ameaças cibernéticas continuam evoluindo, o CIAM pode ser um poderoso aliado na proteção da fronteira digital e no fortalecimento do relacionamento entre o cliente e a empresa.



Hans Vigil Navas
Manager de cibersegurança na NTT DATA Perù

CIBERCRÔNICA

Começamos esta nova edição da RADAR com a seguinte notícia. A Microsoft lançou o alerta após descobrir que um conhecido grupo de hackers ligado ao governo russo tem usado a aplicação Microsoft Teams para realizar ataques de phishing em determinadas organizações.

O grupo, conhecido como "Midnight Blizzard", foi identificado como uma ameaça ligada ao Serviço de Inteligência Externa da Rússia (SVR). Utilizando o Microsoft Teams, os hackers executaram uma campanha de phishing direcionada a alvos em setores governamentais, organizações não governamentais (ONGs), serviços de tecnologia, indústrias e meios de comunicação.

O modus operandi do Midnight Blizzard consiste em usar tenants do Microsoft 365 previamente comprometidos, pertencentes a pequenas empresas, para criar domínios, fazendo-se passar por empresas de suporte técnico confiáveis. Por meio de mensagens no Microsoft Teams, os hackers tentam roubar credenciais de organizações-alvo, solicitando a aprovação da autenticação multifator (MFA) pelos usuários.

> "É fundamental estar sempre atento às táticas de phishing e reforçar as defesas on-line para se proteger contra esses ataques avançados. A colaboração e a vigilância constante são essenciais para combater as crescentes ameaças cibernéticas.".

Os ataques cuidadosamente direcionados afetaram pelo menos 40 organizações em todo o mundo, o que sugere uma operação de espionagem cibernética focada principalmente nos Estados Unidos e na Europa.

Quando os usuários aceitam as mensagens e seguem as instruções, os hackers obtêm credenciais válidas para acessar as contas do Microsoft 365 das vítimas. Em seguida, atividades de roubo de informações foram detectadas nos tenants comprometidos. Além disso, em alguns casos, os hackers tentaram adicionar dispositivos às organizações como dispositivos gerenciados para contornar as políticas de acesso condicional.

A Microsoft tomou medidas para mitigar o uso de domínios por esse grupo e continua investigando outros ataques relacionados.
Esse incidente destaca a importância da conscientização sobre cibersegurança nas organizações. É fundamental estar sempre atento às táticas de phishing e reforçar as defesas on-line para se proteger contra esses ataques avançados. A colaboração e a vigilância constante são essenciais para combater as crescentes ameaças cibernéticas.

Para completar, surge uma nova ferramenta de inteligência artificial (IA) chamada "FraudGPT", voltada especificamente para ataques avançados. Cibercriminosos estão promovendo essa ferramenta em mercados da dark web e canais do Telegram. Projetada para realizar ações criminosas, a ferramenta permite que você crie e-mails do tipo spear phishing, crie um malware não detectável, encontre vulnerabilidades e muito mais. Segundo o criador, houve mais de 3.000 vendas e avaliações confirmadas.

A ferramenta está em circulação desde pelo menos julho de 2023 e é oferecida por meio de um modelo de assinatura que custa US$ 200 por mês, US$ 1.000 por seis meses e US$ 1.700 por um ano. Embora o modelo de linguagem usado para desenvolver o FraudGPT ainda seja desconhecido, essa nova geração de ferramentas de IA para cibercriminosos impõe

desafios significativos à cibersegurança.

Essas ferramentas podem atuar como uma plataforma de lançamento para script kiddies que buscam realizar ataques de phishing corporativo em grande escala, o que poderia resultar em roubo de informações confidenciais e pagamentos não autorizados.

Nesse cenário, torna-se fundamental implementar estratégias de defesa em profundidade e contar com uma rápida telemetria de segurança para detectar e combater ameaças antes que se tornem incidentes de maior gravidade.

Destacamos também a seguinte notícia. De acordo com um relatório da Dragos, uma empresa de cibersegurança industrial, o número de ataques de ransomware a organizações industriais e infraestrutura dobrou desde o segundo trimestre de 2022. No segundo trimestre de 2023, foram registrados 253 incidentes, o que representa um aumento de 18% em relação ao primeiro trimestre do mesmo ano, quando foram observados 214 ataques. A empresa atribui o aumento de ataques a um declínio nas receitas de ransomware em 2022, já que mais vítimas se recusam a fazer o pagamento. Além disso, espera-se que os ataques continuem crescendo devido às tensões políticas entre os países da OTAN e a Rússia, o que motiva os grupos de ransomware associados à Rússia a continuarem atacando infraestruturas críticas em países da OTAN. Também foi observado que os grupos de ransomware estão focados em atacar organizações maiores para garantir suas receitas. O setor de manufatura é o mais afetado, seguido pelos sistemas de controle industrial (ICS, na sigla em inglês), transporte e petróleo e gás.

Um dos ataques mais polêmicos deste mês foi o da CardioComm, uma fornecedora canadense de soluções médicas de monitoramento cardíaco, que foi vítima de um ciberataques que obrigou a empresa a suspender suas operações. Os servidores de produção foram afetados, o que levou à interrupção dos serviços em seu website. A empresa estima que seus negócios serão afetados por vários dias enquanto trabalha para restaurar os dados e os ambientes de servidores.

Embora o ataque não tenha comprometido as informações de saúde dos clientes, a CardioComm tomou precauções para proteger as informações pessoais de seus colaboradores. Acredita-se que o ataque possa ter ocorrido por meio de ransomware, o que levou a empresa a tomar medidas imediatas para conter a situação e evitar maiores danos.

Além disso, esse ciberataque pode trazer consequências financeiras, já que a CardioComm pode enfrentar dificuldades para finalizar o processo necessário devido a uma ordem de suspensão temporária das atividades emitida pela Comissão de Valores Mobiliários de Ontário, que também resultou na suspensão da negociação de suas ações.

A CardioComm é conhecida por fornecer software especializado para registro e análise de eletrocardiogramas, que são usados por hospitais, médicos e dispositivos destinados ao consumidor para diagnosticar pacientes com problemas cardíacos. A empresa está trabalhando arduamente para superar essa situação e restaurar a normalidade das operações.

PODEMOS CONFIAR NOSSA PRIVACIDADE AO CHATGPT?

Por: NTT DATA Europa & Latam

Caso não viva em outro planeta, você saberá o que é o ChatGPT. A parte do “Chat” fica evidente desde o primeiro uso, mas a sigla “GPT” esconde mais do que se imagina.

Generative pre-trained transformers, o ChatGPT é um modelo de Inteligência Artificial (IA) desenvolvido com base na tecnologia OpenAI para a criação de conteúdos (texto ou conversação) e é treinado por meio de uma grande biblioteca que está em constante aprendizado e aprimoramento graças a uma rede neural. O modelo apenas reproduz a maneira de falar dos humanos, aprende com base em muitos textos, porém permanece na camada superficial da semântica e da sintaxe. O sistema também não verifica a confiabilidade das informações e, com toda a desinformação ao nosso redor, isso pode ser perigoso. Da mesma forma, não reconhece o sarcasmo ou o senso de humor.

A IA não funciona sozinha, é necessário um “copiloto”, ou seja, um ser humano. Por que uma máquina precisa ter uma pessoa por trás dela? Para garantir a segurança. Não podemos deixar de reconhecer que estamos no olho de uma tempestade perfeita entre tecnologia e inovação, pois temos à nossa disposição os meios necessários para executar ferramentas como o ChatGPT e, além disso, as condições ideais estão sendo criadas para que esses processos sejam eficientes e para que as decisões de IA tenham relevância e envolvam uma proteção de dados apropriada.

A relação entre a inteligência artificial e as normas de proteção de dados é evidente. Um exemplo disso é que sua política de privacidade não esclarece como são tratados e protegidos os dados pessoais para gerar conteúdo. O que fica explícito é que esses dados são utilizados. O chat é alimentado por uma enorme quantidade de textos coletados na Internet (blogs, artigos, fóruns públicos, websites etc.), portanto, se nossos dados estiverem em qualquer um dos meios mencionados, o ChatGPT terá acesso a eles. Sem mencionar tudo o que o sistema aprende com nossas nuances, a maneira como fazemos perguntas quando interagimos com ele, será que ele faz análises de nós, gera um perfil sem nosso consentimento, é transparente com os usuários?

Por isso, a proteção de dados é extremamente importante para esse tipo de sistema baseado em aprendizagem, e não podemos esquecer os princípios básicos para tornar essas aplicações seguras para o usuário.

Existem 4 pilares essenciais na legislação de proteção de dados:

- Direitos em favor dos titulares dos dados
- Princípios de tratamento de dados (as regras do jogo)
- Medidas proativas de responsabilidade (com base nos riscos)
- Órgãos de controle

A solução mais lógica é estabelecer a política de privacidade desde a concepção. Atuando como um elemento de articulação entre a fase de concepção do sistema de IA e a fase de implantação. Na prática, o elemento-chave é como definimos o sistema de IA. Em muitos casos, se não implantarmos o sistema adequadamente desde a fase de concepção, para que esteja em conformidade com a regulamentação de proteção de dados, mais tarde quando houver uma tomada de decisão, nada poderá ser feito. Quando o sistema for lançado no mercado, se a política de privacidade não tiver sido implementada desde a fase de concepção, esse sistema de IA provavelmente não cumprirá adequadamente as normas de proteção de dados.

O que significa fase de concepção e fase de implantação? Veja abaixo:

FASE DE CONCEPÇÃO DO SISTEMA

- Consolidação do projeto
- Coleta de dados
- Definição de algoritmos
- Desenvolvimento de modelos
- Treinamento de modelos
- Avaliação dos modelos

FASE DE IMPLANTAÇÃO DO SISTEMA

- Organização diferente

(desenvolve/implementa)

- Integração ao ambiente
- Inferências extraídas do modelo
- Tomada de decisões
- Monitoramento do modelo

O primeiro passo ao iniciar um projeto é definir o escopo, os 5Ws (“what”, “who”, “where”, “why”, “when”), para ter um roteiro bem definido. Para que uma IA funcione da maneira que desejamos, é necessário um grande volume de dados para a sua aprendizagem. Quando tivermos esse conjunto de informações sob controle, desenvolveremos, treinaremos e avaliaremos os modelos gerados.

Parece simples, mas é aqui que um dos quatro pilares da proteção de dados entra em ação e, se olharmos atentamente para essas três palavras “coleta de dados”, muitos dos princípios da proteção de dados entram em conflito.

Vamos dar um exemplo para ilustrar melhor. Ao colocarmos a IA em ação e a alimentarmos com um grande volume de dados, o princípio da minimização de dados será, sem dúvida, afetado. Mas, evidentemente, precisamos de vários bancos de dados para que os dados estejam o mais atualizados possível e as variáveis tenham uma representatividade satisfatória. Ao gerar inferências, os dados podem ser imprecisos e não queremos que isso ocorra, de acordo com o princípio da exatidão.

Como executar corretamente os programas que implementam o Privacy by Design do ponto de vista do DPD? É evidente que soluções desse tipo devem ser concebidas em conformidade com a estrutura normativa desde o início. Com a devida justificativa das variáveis escolhidas pelas fases do processo, estabelecendo as finalidades do tratamento, analisando a compatibilidade entre o objetivo inicial e o objetivo final, para que, na fase de implantação do projeto, diferentes equipes entrem em cena - desenvolvedores, controle de qualidade, integradores - e se movimentem dentro dessas margens pré-estabelecidas e possam cumprir as regulamentações.

TENDÊNCIAS

Identidade digital descentralizada: o novo modelo de gerenciamento de identidade em cibersegurança

A identidade digital descentralizada (SSI - Self-Sovereign Identity) é um modelo de gerenciamento de identidade digital que remove a autenticação de uma autoridade única, central e soberana. Em contraste com os modelos tradicionais em que governos e empresas são os detentores da custódia de nossos dados, um sistema de identidade digital descentralizada baseia-se na capacidade do indivíduo de gerenciar e compartilhar suas informações de forma segura e seletiva. Em outras palavras, as funções são intercambiadas, com foco em modelos em que o usuário é quem decide o que pode ou não ser visto sobre nós.

Para obter o autogerenciamento de identidade, teremos que contar com o uso de três pilares básicos:

- **Blockchain**: registro de informações de forma digital e descentralizada, com o uso de criptografia em um blockchain que, por sua estrutura, não permitirá que terceiros consigam modificá-lo.
- **Identidade digital descentralizada** (DIDs, na sigla em inglês): um código único para cada indivíduo, permitindo que ele seja identificado de forma única, assim como gerenciar quais informações gostaria de acessar a partir da carteira (aplicativo ou dispositivo que armazena e gerencia criptomoedas e ativos digitais), na qual as informações são coletadas para sua identificação. Para isso, é realizada uma conexão segura entre duas partes usando um par de chaves públicas e uma ou mais chaves privadas.
- **Credenciais verificáveis** (VCs, na sigla em inglês): as identidades são criptografadas e protegidas para que possam ser verificadas por qualquer organização de forma rápida e eficiente, sem a necessidade de consultar diretamente seus dados pessoais.

O uso de carteira (wallet), mencionado acima, permite que, nesses modelos de SSI, o gerenciamento das informações compartilhadas pelo indivíduo seja inteiramente de sua responsabilidade. Além disso, permite que essa ação seja realizada em qualquer lugar e a qualquer momento, usando um identificador único para essa finalidade. Isso, por sua vez, evitará que sua identidade desapareça se for excluída pelo órgão responsável por seu gerenciamento ou se não for válida em qualquer outro contexto que não seja aquele estabelecido para sua coleta.

Dentro dessa abordagem, encontramos o conceito conhecido como “triângulo de confiança”, composto por: holder (usuário que gera o identificador descentralizado na carteira), issuer (autoridade que emite as credenciais verificáveis) e verifier (parte responsável pela verificação da credencial).

Um exemplo de uso seria em uma solicitação de vaga para uma universidade, em que o aluno (holder) é solicitado a mostrar seu identificador na carteira para provar que possui o diploma de bacharel exigido (cujo issuer seria uma instituição de ensino). Ao compartilhar essas informações, é estabelecida uma conexão segura entre a universidade e o usuário. Somente as informações necessárias são divulgadas, mantendo-se a privacidade de outros dados pessoais, que não são divulgados porque o usuário define o que pode ser consultado. A universidade (verifier) verifica a autenticidade dos dados usando a identidade digital e a chave pública associada armazenada no blockchain.

Essa abordagem de gerenciamento de identidade é mais segura e eficiente do que os métodos tradicionais, evitando a centralização e os riscos de roubo de credenciais. O usuário tem o poder de decidir quem acessa suas informações, reduzindo o risco de escalonamento de privilégios e monitoramento não autorizado. A identidade digital descentralizada e as credenciais verificáveis representam um avanço significativo na proteção da identidade digital e da privacidade em um ambiente cada vez mais digitalizado.

VULNERABILIDADES

Receba nosso boletim informativo completo e de vulnerabilidade inscrevendo-se aqui.

Citrix

CVE-2023-3519, CVE-2023-3466 e CVE-2023-3467
Data: 18/07/2023

Descrição. Foram publicadas três vulnerabilidades relacionadas aos produtos da Citrix (NetScaler ADC e Citrix Gateway). Uma vulnerabilidade é de gravidade crítica (CVE-2023-3519) e as outras duas são de gravidade alta (CVE-2023-3466 e CVE-3467).

- A vulnerabilidade crítica (CVE-2023-3519) explora uma falha que permite a injeção de código e, portanto, a execução de código remoto via acesso não autorizado. A exploração dessa vulnerabilidade exige que o dispositivo seja configurado como um gateway.
- A primeira vulnerabilidades alta (CVE-2023-3466) envolve a possibilidade de execução de ataques de script entre sites (XSS) em decorrência da falta de validação dos dados de entrada. A exploração bem-sucedida dessa vulnerabilidade exige que o invasor envie um URL para a vítima.
- A segunda vulnerabilidade alta (CVE-2023-3467) explora o gerenciamento inadequado de privilégios, permitindo o escalonamento de privilégios dentro do produto vulnerável.

Link: 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

Produtos afetados: Os produtos afetados são:

- NetScaler ADC e NetScaler Gateway 13.1 anteriores à versão 13.1-49.13
- NetScaler ADC e NetScaler Gateway 13.0 anteriores à versão 13.0-91.13
- NetScaler ADC 13.1-FIPS anteriores à versão 13.1-37.159
- NetScaler ADC 12.1-FIPS anteriores à versão 12.1-55.297
- NetScaler ADC 12.1-NDcPP anteriores à versão 12.1-55.297

Solução:
O fabricante propõe como solução a atualização para as seguintes versões:

- NetScaler ADC e NetScaler Gateway 13.1-49.13 e versões posteriores
- NetScaler ADC e NetScaler Gateway 13.0-91.13 e versões posteriores da 13.0
- NetScaler ADC 13.1-FIPS 13.1-37.159 e versões posteriores do 13.1-FIPS
- NetScaler ADC 12.1-FIPS 12.1-55.297 e versões posteriores 12.1-FIPS
- NetScaler ADC 12.1-NDcPP 12.1-55.297 e versões posteriores da 12.1-NDcPP

Ivanti EPMM

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

Descrição. Em julho passado, foram publicadas diversas vulnerabilidades relacionadas ao Ivanti EPMM. Essas vulnerabilidades foram corrigidas com uma série de patches de segurança. No entanto, um grupo de especialistas em cibersegurança detectou uma maneira de contornar as medidas de segurança aplicadas pelo fabricante, expondo novamente as vulnerabilidades.
A nova vulnerabilidade de gravidade crítica (CVE-2023-35082) tem a mesma origem que a anterior (CVE-2023-35078) e pode permitir que um invasor acesse informações de identificação pessoal dos usuários e faça alterações no servidor.
Em especial, um invasor com acesso a diferentes caminhos de API pode acessar informações de identificação pessoal (PII), como nomes, números de telefone e outros dados de dispositivos móveis de usuários contidos em um sistema vulnerável.
Link: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/
Produtos afetados. A vulnerabilidade abrange todas as versões compatíveis (11.4, 11.10, 11.9, 11.8 e anteriores).
Solução: Até o momento, não há previsão de lançamento de novos patches pelo fabricante para corrigir definitivamente essas vulnerabilidades.

PATCHES

Oracle

Data: 19-07-2023

Descrição. A Oracle lançou uma série de atualizações para corrigir 508 vulnerabilidades, incluindo um total de 76 atualizações críticas e 183 CVEs exclusivos. Alguns dos produtos com mais patches e vulnerabilidades críticas estão listados abaixo:

- O produto Oracle Construction and Engineering tem um total de 147 correções e, além disso, 115 exploits remotos sem autenticação. Os patches desse produto aplicam-se aos CVEs: CVE-2023-1370, CVE-2023-24998 e CVE-2022-48285, entre outros.
- O produto Oracle Fusion Middleware tem 60 novos patches de segurança e 40 dessas vulnerabilidades podem ser exploradas remotamente sem autenticação. Alguns dos CVEs relacionados são: CVE-2022-42920, CVE-2022-45047, CVE-2023-25690, CVE-2021-42575 e CVE-2022-41853.
- O produto Oracle MySQL recebeu 24 novas atualizações de segurança. Entre as vulnerabilidades, 11 delas podem ser exploradas remotamente sem autenticação. O CVE mais crítico que foi corrigido com as atualizações de segurança é o CVE-2023-20862.

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

Produtos afetados: Foram afetados 32 produtos diferentes da Oracle

Solução: Aplicar os patches recomendados pela Oracle, de acordo com o produto afetado.

Atlassian

Data: 06/06/2023

Descrição. A Atlassian lançou vários patches de segurança para seus produtos. Esses patches corrigem três vulnerabilidades de gravidade alta. Essas vulnerabilidades podem permitir que um invasor execute as seguintes ações: Essas vulnerabilidades podem permitir que um invasor execute as seguintes ações:

- Execução de código remoto. Essa vulnerabilidade permite que um invasor autenticado execute um código arbitrário com alto impacto de confidencialidade, alto impacto de integridade, alto impacto de disponibilidade e sem interação com o usuário (CVE-2023-22505).
- Essa vulnerabilidade permite que um invasor autenticado execute um código arbitrário com alto impacto sobre a confidencialidade, alto impacto sobre a integridade, alto impacto sobre a disponibilidade e sem interação com o usuário (CVE-2023-22508).
- A injeção e execução de código remoto permite que um invasor autenticado modifique as ações realizadas por uma chamada de sistema e execute um código arbitrário com alto impacto sobre a confidencialidade, alto impacto sobre a integridade, alto impacto sobre a disponibilidade e sem interação com o usuário (CVE-2023-22506).

Link: 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

Produtos afetados: Alguns dos produtos afetados:

- Confluence Data Center & Server.
- Bamboo.

Solução: Aplicar os patches e atualizações publicados no site oficial do fabricante para cada um dos produtos afetados.

EVENTOS

Congresso de cibersegurança no setor de Saúde 5.0

19 de Setembro de 2023

Madri receberá um evento de segurança que será realizado presencial e virtualmente, com o objetivo de conectar os campos de conhecimento de saúde e cibersegurança, visando fortalecer a colaboração de todos os envolvidos na proteção de informações no setor de Saúde. Durante o congresso, serão abordados os diversos desafios que a digitalização do setor de saúde trará do ponto de vista da cibersegurança, como a aplicação de regulamentações, os problemas relacionados a dispositivos médicos conectados remotamente e o aprimoramento da resiliência no setor.

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

Cyber Security & Cloud Expo 2023

26 e 27 de Setembro de 2023

Nos dias 26 e 27 de setembro, será realizado em Amsterdã um evento que contará com palestras de CISOs e discussões sobre questões atuais de cibersegurança em ambientes de nuvem, gerenciamento de riscos, resiliência cibernética, privacidade e regulamentação, gerenciamento de identidade, entre outros tópicos.

Link: - Cyber Security & Cloud Expo 2023 | Technology Conference | Amsterdam (cybersecuritycloudexpo.com)

Gartner Security & Risk Management Summit

26 e 28 de Setembro de 2023

A Conferência Gartner será realizada em Londres, com foco no gerenciamento de riscos para profissionais de segurança, e abordará as possibilidades de fortalecer a cibersegurança, alinhando-a às estratégias de negócios das empresas, gerando um ambiente mais flexível e dinâmico para melhorar os recursos de segurança em ambientes digitais.

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

RECURSOS

Relatório anual de vulnerabilidades de dia zero para Android - Google

O Google publicou seu relatório anual detalhando as vulnerabilidades de dia zero detectadas no Android, utilizadas por cibercriminosos. Desde que esses relatórios começaram a ser publicados em 2014, este ano foi o segundo com o maior número de vulnerabilidades de dia zero detectadas. Entre outras conclusões, o relatório destaca como, devido ao fato de os fabricantes não terem patches de segurança disponíveis a tempo, as vulnerabilidades que foram corrigidas podem ser usadas como vulnerabilidades de dia zero contra os usuários, já que eles não podem fazer as atualizações necessárias em seus dispositivos.

LInk: - Google Online Security Blog: The Ups and Downs of 0-days: A Year in Review of 0-days Exploited In-the-Wild in 2022 (googleblog.com)

BlackLotus

O BlackLotus é um kit de inicialização UEFI projetado especificamente para o Windows, com o objetivo de funcionar como um carregador de HTTP. Essa ferramenta incorpora um bypass de inicialização segura integrado, assim como proteção Ring0/Kernel para evitar qualquer tentativa de remoção depois de implantado. Esse software consiste em dois componentes principais: um agente, que é instalado no dispositivo de destino, e uma interface Web, utilizada pelos administradores para gerenciar os dispositivos instalados pelo agente. Embora esse ataque tenha aparecido em fóruns no ano passado, seu código-fonte foi lançado este mês e agora está acessível a qualquer usuário.

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

Letscall

O Letscall é um novo kit de ferramentas que apresenta uma estrutura fácil de usar para desenvolver e executar ataques de Vishing (Voice over IP Phishing). Esse conjunto apresenta todas as instruções e ferramentas que não apenas descrevem como operar os dispositivos afetados, mas também como se comunicar com as possíveis vítimas. Essa ferramenta já foi usada em lugares como a Coreia do Sul, onde o ataque ocorreu em um assalto a banco.

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

WormGPT

Surgiu uma nova ferramenta chamada FraudGPT, fornecida atualmente apenas via Telegram e que é a sucessora da já conhecida WormGPT. Tanto o FraudGPT quanto o WormGPT fornecem um serviço de inteligência artificial para projetar e desenvolver malware. O serviço é similar ao ChatGPT, porém direcionado à criação de malware, oferecendo um serviço sem restrições e nem limitações éticas. Embora o novo serviço FraudGPT ainda não esteja disponível, já é possível adquirir a ferramenta que o antecedeu, o WormGPT.

Link: https://wormgpt.co/

RESPONSABLES CIBER

María Pilar Torres Bruna

Directora de Cibersegurança en NTT DATA Latam y Perú

maria.pilar.torres.bruna@emeal.nttdata.com

Carla Passos Schwarzer

Directora de Cibersegurança en NTT DATA Brasil

marcelo.nascimento.junior@emeal.nttdata.com

Javier Mauricio Albarracin

Director de Cibersegurança en NTT DATA Colombia

javier.mauricio.albarracin.almanza@emeal.nttdata.com

Fernando Vilchis

Director de Cibersegurança en NTT DATA México

fernando.vilchisrivero@emeal.nttdata.com

Nestor Gerardo Ordoñez

Manager de Cibersegurança en NTT DATA EE.UU

nestor.ordonez.ramirez@emeal.nttdata.com

Carolina Pizarro

Director de Cibersegurança en NTT DATA Chile

carolina.pizarrodiaz@emeal.nttdata.com

Ou escreva para nossa caixa de correio principal: ciberseguridad_latam@emeal.nttdata.com


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