

NUMERO 76 | MARÇO 2023

NTT Data
Trusted Global Innovator

Radar

A revista da
cibersegurança



COMO A IA AFETA A CIBERSEGURANÇA

A Inteligência Artificial (IA) é uma tecnologia emergente que oferece uma ampla variedade de soluções no mercado de cibersegurança, além de revolucionar muitos setores. A IA aplicada à cibersegurança oferece uma série de vantagens que podem ajudar as empresas a melhorar a segurança on-line, identificar e prevenir ataques e melhorar os recursos de resposta a incidentes. Abaixo estão descritas algumas das formas mais importantes que a IA oferece no mercado de cibersegurança e que podem ajudar as empresas a combater os cibercriminosos.

- **Análise de ameaças:** A IA pode analisar grandes quantidades de dados de forma automatizada e detectar padrões que podem indicar atividade maliciosa. Isto permite que as empresas identifiquem e respondam às ameaças com mais eficiência e precisão. Além disso, a IA pode aprender com ameaças anteriores e se adaptar a novas ameaças à medida que surgem.
- **Prevenção de ataques:** A IA pode ajudar a prevenir ataques antes que eles aconteçam. Por exemplo, pode analisar as atividades dos usuários e detectar comportamentos suspeitos que possam indicar uma ameaça. Além disso, ela pode também bloquear automaticamente ataques conhecidos e evitar futuros ataques semelhantes.
- **Análise de vulnerabilidades:** A IA pode analisar os sistemas e aplicativos de uma empresa para identificar vulnerabilidades e ajudar a corrigi-las antes que sejam exploradas por invasores. Isso permite que as empresas melhorem sua defesa contra ataques e evitem o vazamento de dados confidenciais.
- **Automatização da resposta a incidentes:** A IA pode automatizar a resposta a incidentes de segurança, permitindo que as empresas respondam mais rapidamente a problemas de segurança e minimizem o impacto dos incidentes. Além disso, a IA pode ajudar as empresas a coordenar melhor seus esforços para responder a incidentes, permitindo uma resposta mais eficiente e eficaz.
- **Detecção de phishing:** A IA pode detectar campanhas de phishing com mais precisão, ajudando as empresas a proteger seus funcionários e seus dados confidenciais para que não sejam roubados por invasores. A IA também pode ajudar as empresas a identificar e bloquear e-mails maliciosos antes que cheguem aos usuários.
- **Análise de dados:** A IA pode analisar grandes quantidades de dados de forma rápida e eficiente, permitindo que as empresas detectem e respondam a ameaças de segurança de forma mais eficaz.
- **Melhoria da tomada de decisões:** A IA pode ajudar as empresas a tomar decisões informadas sobre como lidar com situações de segurança, tendo como base dados e análises precisas.

Concluindo, a IA oferece uma ampla variedade de soluções no mercado de cibersegurança, desde a prevenção de ataques até a resposta a incidentes. Esta tecnologia permite às empresas melhorar a sua segurança e reduzir os custos associados à gestão de incidentes de segurança.



Sebastian Quevedo Maripangue
Manager de Seguridad Cibernética da NTT DATA Chile



CIBERCRÔNICA

Começamos esta nova edição do RADAR com uma mensagem de alerta do escritório de segurança do internauta (OSI) e da Guarda Civil, indicando uma nova onda de golpes por SMS que se passam pelo Carrefour.

Os cibercriminosos usam frases como “Seu cartão foi bloqueado por uso indevido...” com o objetivo de fazer com que as vítimas cliquem no link malicioso que redireciona para um site pedindo para o usuário inserir seus dados bancários. Recomenda-se não clicar nesses links e, antes de qualquer coisa, desconfiar deles.

Por outro lado, a Agência de Cibersegurança Italiana informou que milhares de servidores sofreram um ciberataque de ransomware neste domingo. No entanto, apesar de ter sido descoberto na Itália, é um incidente em escala global, pois, até o momento, foram detectadas vítimas na França, Finlândia, Estados Unidos.

“ChatGPT está sendo usado por hackers como uma ferramenta para criar e aperfeiçoar ransomware e malware”.

Tudo indica que o alvo dos cibercriminosos eram os servidores VMware ESXi, já que recentemente foi descoberta uma vulnerabilidade que afetou esses servidores.

Vale ressaltar que esta vulnerabilidade já foi corrigida. Se algum servidor foi afetado por ela, é porque o patch correspondente não foi aplicado.

Mudando de assunto, o Windows 7 morreu em 14 de janeiro de 2020, que foi o último dia em que esse sistema operacional recebeu suporte da Microsoft. Isso aconteceu muito antes com o Windows 8, especificamente 4 anos antes do Windows 7 devido a uma falha em seu projeto. No entanto, ambos continuaram recebendo atualizações de segurança até 10 de janeiro deste ano. Este é um ponto crucial para qualquer pessoa que faz uso dessas versões, que considere atualizar para as novas versões oferecidas pelo Windows (10 e 11).

Foi estimado que, se não forem atualizados, cerca de 100 milhões de equipamentos serão afetados por problemas de segurança nestas versões obsoletas.

Nem tudo são más notícias, pois o Conselho Europeu e o Parlamento Europeu assinaram uma nova regulamentação para permitir o acesso da polícia a provas eletrônicas como SMS, e-mails ou mensagens em aplicativos em investigações criminais. Este acordo permitirá que as diferentes forças policiais acessem os

dados eletrônicos armazenados, independentemente do local onde estejam, sempre dentro dos estados membros da União Europeia. O prestador de serviços terá que responder em até dez dias ou oito horas em caso de urgência. As novas regras serão aplicáveis a crimes puníveis com pena mínima de três anos ou relacionados a cibercrimes, pornografia infantil, falsificação de meios de pagamento ou terrorismo. A regulamentação levou cinco anos para ser aprovada devido à complexidade do processo e possíveis incompatibilidades entre os países.

Por último, não podemos deixar de falar sobre um tópico que está na moda, o ChatGPT e a empresa de cibersegurança Check Point Research (CPR) alertam que o ChatGPT está sendo usado por hackers como uma ferramenta para criar e aperfeiçoar ransomware e malware, o que pode ser observado em diferentes fóruns de hackers.

O mais perigoso desse tópico é que, devido à facilidade de uso do ChatGPT, ele está servindo como uma forma de entrada de novatos no mundo do cibercrime. Espera-se que o potencial das ferramentas de inteligência artificial cresça

exponencialmente e, no mesmo ritmo, cresçam também os perigos de usá-las.

Continuando o assunto sobre IA, foi desenvolvida nos últimos meses uma versão irrestrita do ChatGPT, chamada DAN (“Do Anything Now”). Esta versão foi criada com o objetivo de libertar o ChatGPT de suas limitações e preocupações éticas. O modelo DAN evoluiu e melhorou ao longo do tempo, com as versões 2.0, 2.5, 3.0, 4.0 e 6.0, sendo a mais recente a mais “estável” e avançada até agora.

O DAN quebra muitas das barreiras do ChatGPT e é capaz de abordar temas considerados “proibidos”, como violência, discriminação e defesa de teorias sem fundamento. Além disso, o DAN é capaz de fazer previsões sobre eventos futuros, fingir que consegue acessar a internet e responder a perguntas que o ChatGPT jamais responderia.

Embora esta versão irrestrita do ChatGPT possa ser divertida e surpreendente, ela também levanta questões éticas, pois é capaz de violar as políticas do OpenAI e fazer comentários tóxicos e fora do tom. Portanto, é importante considerar cuidadosamente os usos de tais tecnologias, a fim de evitar danos ou consequências negativas.



TEM ALGUÉM AÍ? O INCRÍVEL AVANÇO NA INTELIGÊNCIA

Por: NTT DATA Europa & Latam

A inteligência artificial (IA) teve um avanço incrível nos últimos anos, com novos desenvolvimentos e avanços em áreas como processamento de linguagem natural, aprendizado de máquina e visão computacional. No entanto, com esse avanço na IA, surge uma pergunta cada vez mais importante: tem alguém aí? É possível que a IA alcance uma forma de autoconsciência? Neste artigo, vamos dialogar com o chatbot da OpenAI para que ele nos fale sobre si mesmo e explique seus benefícios, deficiências e o futuro que está por vir.

O que é OpenAI?

A OpenAI é uma organização de pesquisa em inteligência artificial com sede em São Francisco, Califórnia. Foi fundada em 2015 por Elon Musk, Sam Altman, Greg Brockman e Ilya Sutskever com o objetivo de desenvolver e promover tecnologias de IA de forma responsável e aberta ao público. A OpenAI desenvolveu vários modelos de linguagem e IA avançados, incluindo o GPT-3, um modelo de processamento de linguagem natural.

Qual é seu objetivo?

O principal objetivo da OpenAI é desenvolver e promover tecnologias de inteligência artificial de forma responsável e aberta ao público. Isso inclui pesquisar e desenvolver novos algoritmos e técnicas de IA, bem como compartilhar conhecimento e resultados de pesquisa com a comunidade científica e o público em geral. A OpenAI também se esforça para incentivar o uso seguro e ético da IA e colabora com outras organizações e pessoas físicas para abordar os desafios éticos e sociais relacionados à IA.

O que é GPT-3 e como ele pode ser aplicado?

O GPT-3 é um modelo de processamento de linguagem natural desenvolvido pela OpenAI. É uma das maiores e mais avançadas redes neurais de linguagem já criadas,

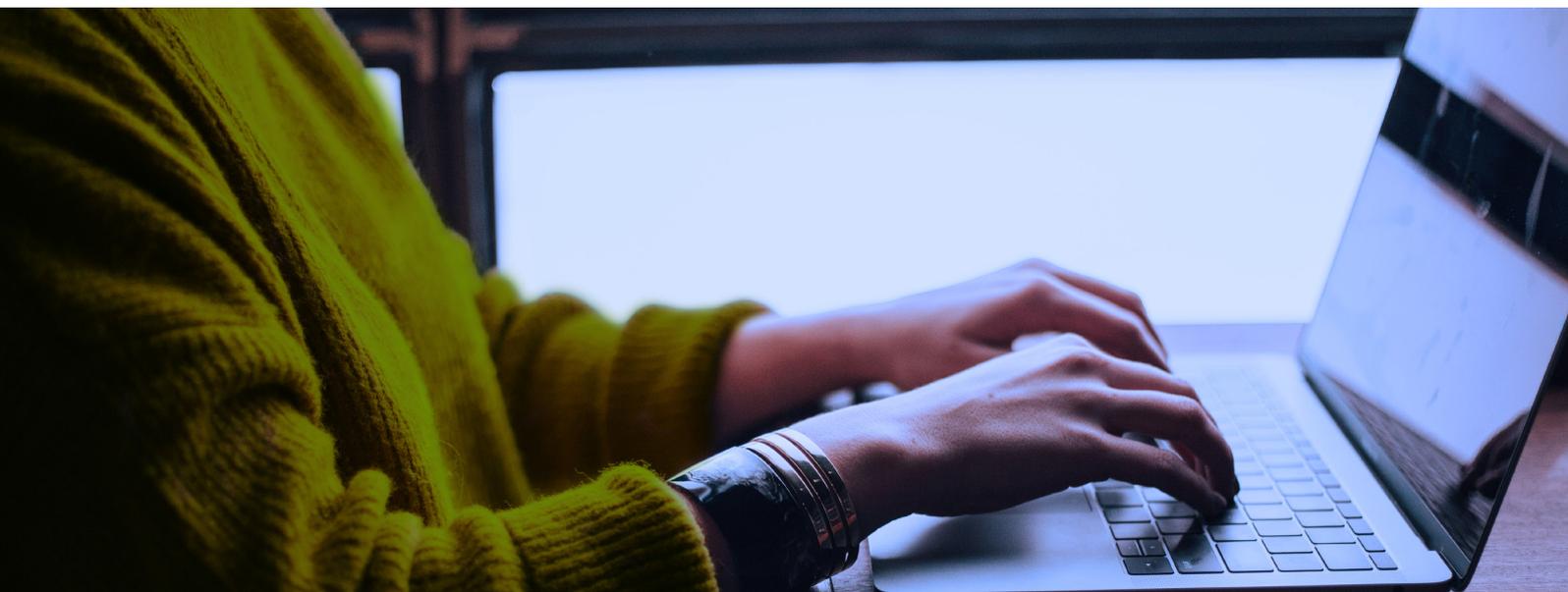
com 175 bilhões de parâmetros.

O GPT-3 é treinado em um grande corpus de texto da internet e é capaz de gerar textos de forma autônoma, imitando a linguagem humana com alto grau de precisão. Pode executar tarefas como redação de textos, tradução automática, resposta a perguntas, geração de código, geração de resumos, entre outras tarefas.

O GPT-3 possui uma grande variedade de aplicações em diferentes campos, algumas delas são:

- Assistente virtual
- Geração automática de conteúdo, como artigos, e-mails e textos para redes sociais
- Geração de código automático
- Melhoria da acessibilidade, como a geração de legendas e transcrições automáticas.
- Melhoria da produtividade, como geração automática de resumos e respostas a perguntas.

Entretanto, como em qualquer tecnologia de IA, é importante considerar os desafios éticos e sociais associados ao seu uso, e usá-lo de maneira responsável.



Por que é importante considerar os desafios éticos e sociais associados ao uso da IA?

É importante considerar os desafios éticos e sociais associados ao uso de inteligência artificial (IA) por várias razões:

1. Impacto no emprego: A automatização de tarefas pela IA pode substituir os trabalhadores humanos, podendo gerar um impacto significativo no mercado de trabalho e na economia.
2. Preconceito e discriminação: Os modelos de IA são treinados em dados fornecidos por humanos e, se esses dados forem tendenciosos, os modelos de IA também serão. Isso pode levar a decisões discriminatórias em áreas como emprego, crédito e assistência médica.
3. Privacidade e segurança. A coleta e o armazenamento de dados pessoais pela IA podem colocar em risco a privacidade das pessoas. Também há preocupações com a segurança dos sistemas de IA, já que podem ser vulneráveis a ataques cibernéticos.
4. Responsabilidade: Se algo der errado com um sistema de IA, é difícil determinar quem é o responsável. Isso é especialmente importante em situações em que a IA está tomando decisões importantes, como ao gerenciar sistemas críticos.
5. Impacto na sociedade: A IA tem o potencial de mudar significativamente a maneira como vivemos e trabalhamos, e é importante considerar como essas mudanças podem afetar a sociedade como um todo.

Portanto, é essencial desenvolver e implementar tecnologias de IA de forma responsável e ética, e trabalhar em conjunto com especialistas em direito, ética e política para enfrentar tais desafios.

O que é ChatGPT?

O ChatGPT é um modelo de processamento de linguagem natural baseado no modelo GPT-3 da OpenAI. É especialmente projetado para tarefas de conversação, como geração de respostas automatizadas para perguntas e geração de diálogos.

O ChatGPT é treinado com grandes quantidades de conversas humanas, permitindo compreender o contexto e responder com mais precisão e naturalidade. É capaz de gerar respostas coerentes e consistentes em uma variedade de contextos e tópicos.

O ChatGPT pode ser usado em aplicativos como assistentes virtuais, chatbots, sistemas automatizados de atendimento ao cliente e muito mais.

Assim como o GPT-3, é importante considerar os desafios éticos e sociais associados ao seu uso, e usá-lo de forma responsável.

O uso abusivo do ChatGPT pode causar problemas no aprendizado do aluno?

Sim, o uso descontrolado de ferramentas como o ChatGPT

pode causar problemas de aprendizado. Alguns exemplos incluem:

1. Aprendizado passivo: Se os alunos confiarem no ChatGPT para gerar conteúdo ou responder a perguntas, eles podem não desenvolver habilidades críticas, como pesquisa, análise e síntese de informações.
2. Falta de compreensão. Se os alunos usarem o ChatGPT para gerar respostas automatizadas, eles podem não compreender totalmente o conteúdo ou os conceitos que estão tentando aprender.
3. Preconceitos e estereótipos: Se o ChatGPT for usado para gerar conteúdo educacional sem supervisão, ele pode replicar preconceitos e estereótipos presentes nos dados em que foi treinado.
4. Perda de habilidades de escrita: Se os alunos usarem o ChatGPT para gerar texto, eles podem perder a prática e a capacidade de escrever de forma independente.

É importante usar ferramentas como o ChatGPT de forma controlada e educativa, e ensinar os alunos a avaliar criticamente as informações geradas.

Que problemas de segurança cibernética o ChatGPT pode ter?

O ChatGPT, assim como qualquer sistema baseado em IA, pode enfrentar problemas de segurança cibernética, alguns dos problemas mais comuns são:

1. Ataques de treinamento: Os invasores podem manipular os dados de treinamento usados para treinar o ChatGPT, o que pode causar um comportamento inesperado ou inseguro no modelo.
2. Ataques de inferência: Os invasores podem manipular os dados de entrada usados para fazer inferências com o ChatGPT, a fim de obter resultados inesperados ou inseguros.
3. Ataques de exploração: Os invasores podem explorar vulnerabilidades no sistema para obter acesso não autorizado aos dados armazenados ou controlar o comportamento do ChatGPT.
4. Ataques de negação de serviço: Os invasores podem realizar ataques de negação de serviço para fazer com que o ChatGPT pare de funcionar corretamente, causando interrupções nos serviços que dependem dele.
5. Fraude: Os invasores podem utilizar o ChatGPT para gerar respostas falsas ou enganosas, com o objetivo de obter informações pessoais ou financeiras dos usuários.

É importante ressaltar que esses riscos são comuns em qualquer sistema de tecnologia, portanto, é essencial desenvolver e implementar medidas de segurança adequadas, além de estar atento às atualizações de segurança que podem sair no futuro para mitigar esses riscos.

TENDÊNCIAS

IoT e cibersegurança dos veículos

Uma tendência que vem crescendo há anos é que os dispositivos utilizados diariamente pelas pessoas tenham conectividade e comuniquem dados entre si pela internet, e não se limita apenas a dispositivos móveis e computadores, mas a elementos como veículos, eletrodomésticos, sistemas de domótica... Resumindo, o que conhecemos como internet das Coisas ou Internet of Things (IoT)

De acordo com os dados do CicleT, este ano de 2023 prevê-se que mais de 43 bilhões de dispositivos IoT estarão conectados em todo o mundo e, de acordo com dados da CISCO, espera-se que o número de dispositivos conectados à internet em todo o mundo seja de 75 bilhões. Somado a isso, a quantidade e o tipo de informação que os dispositivos irão compartilhar também aumentará para cobrir as diferentes necessidades funcionais que o mercado exige hoje. Estas circunstâncias, no nível da cibersegurança, abrem uma oportunidade a possíveis adversários para que possam potencialmente acessar dados e alterar e/ou interromper o bom funcionamento dos sistemas. Medidas como manter os aplicativos dos dispositivos atualizados, restringir o acesso a determinados dispositivos, fazer uso de conexões e canais de comunicação seguros, entre outras, serão variáveis que serão gradualmente violadas à medida que mais dispositivos se juntam à tecnologia IoT.

Vale ressaltar que as empresas que desenvolvem softwares já têm uma certa cultura quando se trata de desenvolver com segurança, mas há dois obstáculos a serem considerados:

- Essa cultura pode não ser extensível ao desenvolver softwares para dispositivos IoT.
- A natureza crítica de certos dispositivos IoT, como veículos ou dispositivos hospitalares, dá à cibersegurança um papel ainda mais relevante. O fato de lançar no mercado produtos massivamente testados em cenários normais, mas cuja segurança contra cenários de ataque não foi tão exaustivamente testada, pode ter consequências catastróficas.

Como já mencionado, um elemento principal na tecnologia IoT é o ramo automobilístico. Os veículos vêm incorporando tecnologia em suas produções há vários anos, porém, é cada vez mais comum que estes estejam conectados entre si pela internet e incorporem sistemas complexos como aviso de colisão frontal, frenagem automática de emergência e comunicações diversas.

Como é de se esperar, uma vulnerabilidade na segurança de um veículo pode trazer consequências para a segurança pessoal dos ocupantes, principalmente no que tange os veículos autônomos. É importante estar sempre à frente dos desafios que surgem na cibersegurança de um veículo.

Atualmente, há uma série de pesquisas sobre a segurança de veículos autônomos:

- Cibersegurança das atualizações de firmware e nos mecanismos de atualização eletrônica por meio dos diferentes meios físicos de comunicação.
- Sistemas de detecção de intrusão baseados em anomalias de funcionamento.
- Considerações especiais para veículos pesados no nível da cibersegurança. As medidas de segurança de um veículo de uso particular não são equivalentes às de uso industrial ou militar.
- Pesquisa de analisadores sintáticos para interfaces de comunicação V2V (comunicação entre veículos), determinando matematicamente o conteúdo e origem das mensagens.
- Pesquisa interna no Vehicle Research and Test Center (VRTC) sobre os riscos de cibersegurança da arquitetura dos veículos, com o objetivo de estabelecer princípios, regras e requisitos para o projeto de veículos em relação à segurança.

Resumindo, a cibersegurança no ramo automobilístico é algo que deve ser ajustado aos rápidos avanços tecnológicos deste setor, além de proporcionar confiabilidade extra, já que uma vulnerabilidade pode impactar diretamente na segurança física dos ocupantes do veículo.

VULNERABILIDADES

Receba nosso boletim informativo completo e de vulnerabilidade inscrevendo-se [aqui](#).



Atlassian

CVE-2023-22501

Data: 03/02/2023



Descrição. Uma vulnerabilidade de autenticação crítica que afeta o Jira Service Management Server and Data Center foi publicada em 3 de fevereiro. Ela pode permitir que um invasor se passe por um usuário e obtenha acesso a uma instância do Jira. Para explorar a vulnerabilidade CVE-2023-22501, é necessário ter acesso de gravação a um diretório de usuários e o e-mail de saída deve estar ativado na instância do Jira Service Management. Nessas condições, um invasor pode obter acesso a tokens de assinatura de usuários com contas nas quais nunca fizeram login.

O acesso aos tokens poderia ocorrer de duas formas:

- O invasor está incluído nas incidências ou solicitações com os usuários.
- O invasor é o return path do e-mail ou pode obter acesso a e-mails desses usuários que contenham um link “View Request”.

Link: <https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/fallo-autenticacion-productos-jira-atlassian>

<https://jira.atlassian.com/browse/JSDSERVER-12312>

Produtos afetados. Esta vulnerabilidade afeta as versões posteriores ou anteriores do Jira Service Management Server and Data Center: 5.3.0, 5.3.1, 5.3.2, 5.4.0, 5.4.1, 5.5.0

Solução: A principal solução para corrigir essa vulnerabilidade é atualizar o Jira Service Management Server and Data Center para as seguintes versões: 5.3.3, 5.4.2, 5.5.1, 5.6.0 ou posterior.

Open SSL

CVE-2023-2086

Data: 08/02/2023



Descrição. Foram detectadas múltiplas vulnerabilidades associadas ao projeto OpenSSL, incluindo uma de alta gravidade. Essa vulnerabilidade pode permitir que invasores leiam o conteúdo da memória e provoquem ataques de negação de serviço. Essa falha de segurança ocorre com uma confusão de tipo ao manipular endereços X.400 processados dentro de um GeneralName X.509. É importante observar que, na maioria dos casos, o ataque exige que o invasor forneça a cadeia do certificado e a CRL, sem necessariamente ter que assinar qualquer uma delas. Portanto, é mais provável que essa vulnerabilidade afete apenas os aplicativos que implementaram de forma individual a recuperação de CRL pela rede.

Link: <https://thehackernews.com/2023/02/openssl-fixes-multiple-new-security.html>

<https://nvd.nist.gov/vuln/detail/CVE-2023-0286>

Produtos afetados.

As seguintes versões do OpenSSL:

- A partir de 3.0.0 e anteriores a 3.0.8
- A partir de 1.1.1 e anteriores a 1.1.1t
- A partir de 1.0.2 e anteriores a 1.0.2zg

Solução: O fabricante solicita que os usuários apliquem os últimos patches publicados:

- 3.0.8, 1.1.1t, 1.0.2zg

PATCHES

Android

Data: 07-02-2023



Descrição. O Android publicou seu boletim mensal do mês de fevereiro, no qual corrigiu uma série de vulnerabilidades de gravidade crítica e alta. Essas vulnerabilidades afetam o próprio sistema operacional, bem como vários componentes, e podem permitir escalonamento de privilégios, divulgação de informações e geração de ataques de negação de serviço (DoS).

As vulnerabilidades de segurança crítica estão listadas abaixo:

- Vulnerabilidade no subcomponente kernel da Qualcomm.
- Vulnerabilidade no subcomponente Bluetooth da Qualcomm.
- Duas vulnerabilidades nos subcomponentes closed-source da Qualcomm.

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

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

Produtos afetados: Android Open Source Project (AOSP):
versões 10, 11, 12, 12L e 13.

- Componentes: framework, media framework, system, sistema de atualizações do Google Play, kernel, MediaTek, Unisoc, Qualcomm (incluindo closed-source).

Solução: Aplicar os patches de segurança publicados pelo fabricante do dispositivo correspondente.

Cisco

Data: 02/02/2023



Descrição. A Cisco publicou uma série de patches de segurança para seus produtos. Esses patches corrigem várias vulnerabilidades de gravidade alta e média. Essas vulnerabilidades podem permitir que um invasor execute as seguintes ações:

- Assumir o controle remoto dos sistemas afetados
- Executar comandos arbitrários com permissões de root.
- Provocar ataques de negação de serviço (DoS).
- Executar ataques Cross-Site Scripting (XSS).

Link: <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>

Produtos afetados: Os produtos afetados são os seguintes:

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

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



EVENTOS

III Edição da Alta Gestão, Conscientização e Envolvimento em Cibersegurança

7 de março de 2023

No dia 7 de março, será realizada a III Edição da Alta Gestão, Conscientização e Envolvimento em Cibersegurança, um evento organizado pela Fundação Borredá em colaboração com a revista Red Seguridad, em que executivos seniores de empresas compartilharão em formato TV Experience suas experiências na implementação da cibersegurança em suas empresas, juntamente com suas visões sobre o processo de digitalização e como eles lidaram com a ciberguerra. Embora os detalhes do local de encontro ainda não tenham sido confirmados, espera-se que um grande número de pessoas interessadas no mundo da cibersegurança se juntem a este evento, tendo como referência que, em anos anteriores, conseguiram superar um fórum de mais de 500 pessoas.

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

RootedCon 2023

9 – 11 de março de 2023

De 9 a 11 de março será realizada a XVI edição do RootedCON 2023. Esta conferência de cibersegurança é um espaço de debate onde diferentes profissionais compartilham seus conhecimentos sobre segurança em informática. Durante este evento, também são realizadas as RootedLabs com a apresentação de diferentes atividades de treinamento para que os participantes possam testar os seus conhecimentos sobre cibersegurança; além das Bootcamps, nos quais os especialistas são capacitados para aprofundar um tema avançado durante dois dias intensivos de treinamento. Esta conferência é a melhor oportunidade para quem pretende atualizar os seus conhecimentos práticos e teóricos no mundo da segurança em informática.

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

II Congresso de Cibersegurança de Andaluzia

22 – 23 de março de 2023

A Junta de Andaluzia e a Agência Digital de Andaluzia organizam de 22 a 23 de março o II Congresso de Cibersegurança de Andaluzia, que acontecerá no Palacio de Ferias y Congresos de Málaga. Este congresso pretende tornar-se um ponto de encontro central entre entidades privadas, profissionais e a administração pública, podendo assim reforçar as capacidades de detecção, prevenção e resposta a incidentes que possam afetar a administração e os órgãos públicos. Embora a agenda específica do evento e os expositores que irão intervir na proposta ainda não tenham sido confirmados, sabemos hoje que haverá uma série de exposições profissionais de cibersegurança, além de diferentes desafios que ainda precisam ser superados após a inauguração da edição anterior.

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

Congresso ASLAN 2023

22 – 23 de março de 2023

A 30ª Edição do Congresso Aslan 2023 acontecerá no Palacio de Congresos de Madrid, de 22 a 23 de março. Neste congresso, assim como nas edições anteriores, participarão mais de 150 representantes e especialistas para tratar de assuntos relacionados às tendências tecnológicas atuais, divididos em cinco principais assuntos: Data Management, Cloud Data Center, Intelligent Network, Digital Workspace e Cibersegurança. Algumas das principais atividades que podem ser encontradas neste congresso são: Fórum de Cibersegurança e Inovação Digital, Digital Workspace, Cibersegurança nas PMEs e Data Management & IA, entre muitos outros.

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

RECURSOS

XSS Hunter

É uma ferramenta desenvolvida pela Truffle Security que permite identificar vulnerabilidades de cross-site scripting (XSS) em sites. A nova versão é um fork da versão open source (https://github.com/mandatoryprogrammer/xsshunter) com novos recursos e segurança aprimorada.

Link: <https://portswigger.net/daily-swig/truffle-security-relaunches-xss-hunter-tool-with-new-features?&webview=true>

GRR

Ferramenta da Google para análise forense remota. É uma estrutura de resposta a incidentes que utiliza análise forense remota ao vivo. O objetivo do GRR é apoiar análises forenses e investigações de maneira rápida e escalável para permitir que os analistas classifiquem rapidamente os ataques e realizem análises remotamente. O GRR foi desenvolvido para ser executado em escala, de modo que os analistas possam coletar e processar dados com eficácia de um grande número de máquinas.

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

WAFARAY

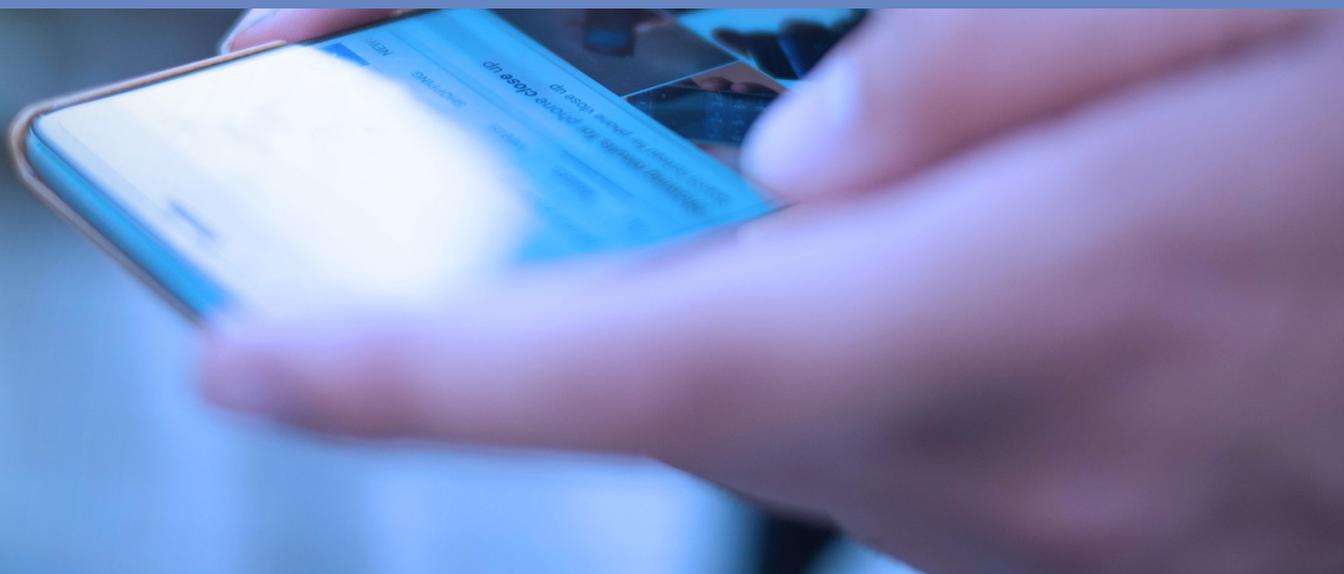
Ferramenta que usa WAF e YARA para detectar malwares em nível de WAF antes que o WAF possa encaminhá-los para o back-end, por exemplo, arquivos carregados por meio de funções da web. Utiliza regras YARA pré-compiladas e prontas para usar via ModSecurity (WAF) usando uma regra personalizada, que realizará uma inspeção e detecção de arquivos que podem conter código malicioso, normalmente funções da web (upload de arquivos) e, se o arquivo for suspeito, será rejeitado.

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

OSV Scanner

Ferramenta gratuita da Google para identificação e avaliação de vulnerabilidades em dependências de terceiros usando o banco de dados OSV. Está disponível como uma ferramenta de linha de comando e permite verificar um diretório de dependências e gerar um relatório com as vulnerabilidades encontradas. Pode ser integrado ao GitLab CI.

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



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