TRUSTED FUTURE

HIT EM FOCO

UMA ANÁLISE SOBRE A PRIMEIRA SOLICITAÇÃO DE INTEROPERABILIDADE DO DMA

→ **O acesso irrestrito a recursos fundamentais de compilação just-in-time, ou o uso de JIT de forma insegura, cria vulnerabilidades significativas que podem ser facilmente exploradas pelos hackers.**

À medida que a União Europeia (UE) implementa a Lei dos Mercados Digitais (DMA), seus mandatos se deparam com uma dura realidade técnica: algumas dessas regulamentações estão, na verdade, enfraquecendo a segurança cibernética. Um novo artigo de Jim Kohlenberger, da Trusted Future, analisa como os requisitos de interoperabilidade estão expondo vulnerabilidades de segurança importantes e pede que os responsáveis pela aplicação do DMA garantam que seus requisitos não exponham involuntariamente os usuários a um risco de segurança maior.

O QUE ACONTECEU?

- A Lei de Mercados Digitais da UE exige que as grandes empresas digitais, aquelas que são identificadas como "gatekeepers" (ou controladora de acessos), garantam que seus softwares e hardwares sejam interoperáveis com desenvolvedores terceiros.
- A primeira solicitação de interoperabilidade enviada publicamente por um desenvolvedor pede que a Apple forneça acesso direto aos recursos do seu compilador Just-In-Time, ou mecanismo JIT.
- Isso nos dá a primeira oportunidade de avaliar como a regulamentação da concorrência da UE está realmente afetando a segurança cibernética em um cenário real.

POR QUE A INTEROPERABILIDADE É IMPORTANTE?

- A interoperabilidade no mundo digital pode trazer grandes benefícios para consumidores e empresas.
- As ferramentas de interoperabilidade incorporadas aos smartphones permitiram que milhões de aplicativos de terceiros funcionassem com sensores integrados, capacidade de computação e serviços de conectividade de um dispositivo, o que ajudou a viabilizar um ecossistema de aplicativos e dispositivos de terceiros conectados.
- Até agora, essa interoperabilidade gerou amplos benefícios econômicos, em parte porque foram habilitados com salvaguardas incorporadas para proteger a segurança e a privacidade dos usuários.
- Mas a interoperabilidade obrigatória pode ser problemática quando feita de forma a prejudicar ou minar essas proteções e colocar em risco a privacidade, a segurança e a proteção fundamentais dos consumidores.

O QUE É JIT?

- Um compilador Just-In-Time ou mecanismo JIT é o software usado pelos navegadores para compilar o código de uma linguagem baseada na web para a linguagem que o sistema operacional do smartphone entende. É uma função crucial, necessária e obrigatória para que os navegadores funcionem de forma rápida e eficiente. Mas também é altamente complexo.
- O JIT é uma técnica fundamental usada em navegadores modernos que permite que os usuários acessem sites interativos complexos, como jogos, Gmail, Instagram, TikTok e muitos outros, para que sejam executados de forma mais rápida, eficiente e estável.
- A função JIT permite que esses sites complexos sejam executados de forma significativamente mais eficiente, usando uma

série de pipelines complexos para compilar ou traduzir o código JavaScript de sites, baseado em texto, em um código de máquina mais eficiente, que pode ser executado de forma mais rápida em um sistema operacional.

- Esses mecanismos JIT, agora usados em todos os principais navegadores, podem obter ganhos de desempenho bastante impressionantes. Mas esses ganhos vêm acompanhados de riscos adicionais de segurança: Um dos principais recursos que ajudam a possibilitar esses ganhos impressionantes é que um mecanismo JIT pode gravar dados na memória e, posteriormente, executar essa memória como código.
- Os mecanismos JIT se tornaram o principal alvo dos hackers porque:
  - Representam cerca de metade das explorações de navegador
  - São difíceis de depurar
  - Podem levar à execução arbitrária do código
  - Têm brechas extremas que são muito prejudiciais
- Já sabemos as consequências para o mundo real: O JIT esteve envolvido na obtenção de amplo controle de um telefone através da brecha original do spyware mercenário Pegasus como parte de uma cadeia sofisticada para inserir o malware na parte de leitura/gravação/execução de um smartphone.

QUAIS SÃO AS INFORMAÇÕES DA SOLICITAÇÃO DE INTEROPERABILIDADE?

- Nessa solicitação, a primeira publicada no âmbito do DMA, um desenvolvedor está solicitando acesso a uma interface de programação de aplicativos (API - ou a forma como os programas de software comunicam solicitações e respostas entre si) para ajudar a fazer com que seu aplicativo emulador de Linux seja executado com uma ordem de magnitude mais rápida, mais eficiente e usando menos energia, o que pode prolongar a vida útil da bateria - um dos principais benefícios que as regras de interoperabilidade do DMA pretendem possibilitar.
- A Apple criou uma API de habilitação de JIT para atender outra parte do DMA e permitir que os desenvolvedores de navegadores confiáveis ofereçam seus próprios navegadores com mecanismos de JIT próprios. Mas, de acordo com o DMA, o desenvolvedor pode solicitar acesso igual ao mecanismo JIT da Apple, já que os regulamentos exigem que "a interoperabilidade deve ser concedida ao mesmo recurso em condições iguais".

POR QUE ISSO É IMPORTANTE?

- Embora o desenvolvedor esteja seguindo as etapas descritas no DMA e, em sua opinião, fazendo uma solicitação que se encaixa no objetivo das regras do DMA, isso expõe uma tensão inerente ao regulamento do DMA. Mas forçar a Apple a abrir o acesso direto de leitura/gravação/execução do JIT para qualquer pessoa poderia mudar fundamentalmente o cálculo de segurança para os usuários do iPhone.
- Se a Apple fosse forçada a abrir esse recurso para qualquer desenvolvedor, isso poderia levar a novos riscos de segurança sem precedentes, dar uma vantagem aos agentes que ameaçam estados e nações e colocar em risco a integridade das principais operações de negócios da empresa.
- Isso poderia expandir significativamente os riscos cibernéticos para 82% das organizações europeias que utilizam plataformas móveis no local de trabalho.
- Os responsáveis pela aplicação da DMA devem reconsiderar esses mandatos de interoperabilidade e garantir que seus requisitos não exponham involuntariamente os usuários a maiores riscos de segurança. E é um alerta para criação de políticas que queiram replicar aquelas semelhantes às do DMA.

→ **LEIA MAIS AQUI**