TRUSTED FUTURE

JIT HAPPENS

A LOOK AT THE DMA'S FIRST INTEROPERABILITY REQUEST

→ **Unfettered access to fundamental just-in-time compiling features, or use of insecure JIT, creates significant vulnerabilities that hackers can easily exploit.**

As the European Union (EU) implements the Digital Markets Act (DMA), its mandates are meeting a harsh technical reality: some of these regulations are actually weakening cybersecurity. A new brief by Trusted Future's Jim Kohlenberger takes a look at how interoperability requirements are exposing serious security vulnerabilities, and urges the DMA's enforcers to ensure that its requirements do not unintentionally expose users to higher security risk.

WHAT HAPPENED?

- The EU's Digital Markets Act requires large digital companies – those they identify as "gatekeepers" – to ensure their software and hardware are interoperable with third-party developers.
- The first interoperability request publicly posted by a developer requests Apple provide it with direct access to features of its Just-In-Time Compiler, or JIT engine.
- This provides us with the first opportunity to evaluate how the EU's competition regulation is actually impacting cybersecurity in a real-life scenario.

WHY DOES INTEROPERABILITY MATTER?

- Interoperability in the digital world can bring enormous benefits for consumers and businesses.
- The interoperability tools built into smartphones have enabled millions of third-party apps to work with a device's on-board sensors, computing power, and connectivity services, which have helped enable an ecosystem of third party connected apps and devices.
- Until now, this interoperability created broad economic benefits in part because they have been enabled with safeguards built in to protect the safety, security, and privacy of all users.
- But mandated interoperability can be problematic when it is done in a way that harms or undermines these safeguards and puts consumers' fundamental privacy, safety, and security at risk.

WHAT IS JIT?

- A Just-In-Time compiler or JIT engine is the software used by web browsers to compile code from a web-based language to the language the operating system of the smartphone understands. It is a crucial, necessary, and required function to make web browsers work fast and efficiently. It is also highly complex.
- JIT is a foundational technique used in modern browsers that enables users to access complex interactive websites like games, Gmail, Instagram, TikTok, and millions of others to run faster, more efficiently, and more smoothly.

- The JIT function enables these complex websites to run significantly more efficiently by taking the text-based JavaScript code from the webpage and, through a series of complex pipelines, compiles or translates the code into a more efficient machine code that can run faster in an operating system.
- These JIT engines – which are now used in every major browser – can achieve quite impressive performance gains. But these performance gains come with added security risks: one of the key features that helps enable these impressive gains is that a JIT engine is allowed to both write to memory and later execute that memory as code.
- JIT engines have become a primary target of hackers because they:
  - Account for roughly one half of browser exploits
  - Are difficult to debug
  - Can lead to arbitrary code execution
  - Have exploits that are very harmful and extreme
- We already know the real-world consequences: JIT was involved in gaining broad control of a phone in the original Pegasus mercenary spyware exploit as part of a sophisticated chain to mainline malware into the read/write/execute part of a smartphone.

WHAT ARE THE DETAILS OF THE INTEROPERABILITY REQUEST?

- In this request, the first published under the DMA, a developer is asking for access to an application programming interface (API – or the way that software programs can communicate requests and responses with each other) to help make its Linux emulator app run an order of magnitude faster, more efficiently, and utilize less power which can extend battery life – the kind of key benefits that DMA interoperability rules are intended to enable.
- Apple built a JIT enabling API to comply with another part of the DMA to allow trusted browser developers the ability to offer their own web browsers with their own JIT engines. But under the DMA, the developer is allowed to request equal access to Apple's own JIT engine, as the regulations broadly require "interoperability must be granted to the same feature under equal conditions."

WHY DOES THIS MATTER?

- While the developer is following the steps outlined under the DMA, and in its view seeking what the DMA's rules are designed to address, it exposes an inherent tension in the DMA regulation. By forcing Apple to open up the JIT's direct read/write/execute access to anyone, the DMA will fundamentally change the security calculus for iPhone users.
- If Apple were forced to open up this feature to any developer, it could lead to unprecedented new security risks, give nation state threat actors a leg up, and put the integrity of core enterprise business operations at risk. This could potentially expand significant cyber risks to the 82% of European organizations that leverage mobile platforms in the workplace.
- The DMA's enforcers should reconsider these interoperability mandates and ensure that its requirements do not unintentionally expose users to higher security risks.
- It's a red flag warning to any policymakers looking to replicate DMA-like policies.

→ **READ MORE HERE**