TRUSTED FUTURE

迫る JIT

DMA初の相互運用性要求の考察

→ 重要なジャストインタイムのコンパイル機能へのアクセスに制限がなかったり、安全でないJITを使用したりすると、ハッカーが容易に悪用できる深刻な脆弱性が生じます。

欧州連合（EU）がデジタル市場法（DMA）を実施する中、その命令は厳しい技術的現実に直面しています。これらの規制の中には、サイバーセキュリティを事実上弱体化させているものもあります。Trusted FutureのJim Kohlenberger氏による新しい報告書では、相互運用性要件がいかに深刻なセキュリティの脆弱性を露呈しているかを取り上げ、DMAの執行者に対し、その要件によりユーザーが意図せずより高いセキュリティリスクにさらされることがないようにすることを強く求めています。

これまでの経緯

- EUのデジタル市場法は、大手デジタル企業（「ゲートキーパー」と指定される企業）に対し、各社のソフトウェアやハードウェアが、第三者のデベロッパーと相互運用可能であるようにすることを求めています。
- デベロッパーから公に投稿された最初の相互運用性に関する要求では、デベロッパーがAppleに対し、ジャストインタイムコンパイラ（JITエンジン）の機能に直接アクセスできるようにすることを求めています。
- これは、EUの競争規制が、現実世界のシナリオにおいてサイバーセキュリティにどのような影響を及ぼしているのかを私たちが評価できる初めての機会となります。

相互運用性が重要である理由

- デジタルの世界における相互運用性の実現により、消費者と企業に非常に大きなメリットがもたらされます。
- スマートフォンに組み込まれた相互運用性ツールは、何百万ものサードパーティ製アプリがオンボードのセンサーや演算能力、コネクティビティサービスを活用できるようにし、それによってサードパーティの接続アプリやデバイスのエコシステムが実現しました。
- これまで、この相互運用性が幅広い経済的利益をもたらした理由の一部として、すべてのユーザーの安全、セキュリティ、プライバシーを保護するために安全策が組み込まれていたことがありました。
- しかし、相互運用性の義務化が、これらの安全策に害を与えたり効果を弱めたりし、あるいは消費者の基本的なプライバシー、安全、セキュリティを危険にさらすような形で行われると、問題が生じる可能性があります。

JITとは

- ジャストインタイムコンパイラ（JITエンジン）は、Webベースの言語を、スマートフォンのオペレーティングシステムが理解できる言語へとコードをコンパイルするために、Webブラウザが使用するソフトウェアです。これは、Webブラウザを高速かつ効率的に動作させるために不可欠で、必要かつ必須の機能です。また、非常に複雑でもあります。
- JITは、最新のブラウザで使用されている基礎的な技術です。ゲーム、Gmail、Instagram、TikTok、その他何百万もの複雑でインタラクティブなWebサイトにユーザーがアクセスできるようにし、高速かつ効率的に、スムーズに動作するようにします。
- JIT機能により、これらの複雑なWebサイトを極めて効率的に動作できるようになります。Webページからテキストベースの JavaScriptコードを取得し、一連の複雑なパイプラインを通じて、オペレーティングシステムで高速に実行できる、より効率的な機械語へとコードをコンパイルまたは変換します。

- このようなJITエンジンは、現在ではあらゆる主要ブラウザで使用されており、パフォーマンスを目覚ましく向上させることができます。しかし、こうしたパフォーマンス向上には、セキュリティ上のリスクが伴います。こうした大幅な進歩を可能としている主な機能のひとつとして、JITエンジンは、メモリへの書き込みと、そのメモリを後にコードとして実行できることがあります。
- JITエンジンは、ハッカーの主要な標的となっていますが、それには次のような理由があります。
  - ブラウザのエクスプロイト攻撃の約半数を占めている
  - デバッグが難しい
  - 任意のコード実行につながる恐れがある
  - 極めて有害で極端なエクスプロイトを持つ
    私たちはすでに現実世界における結果を知っています。JITは、スマートフォンの読み取り/書き込み/実行部分にマルウェアを仕込む巧妙なチェーンの一部として、元のPegasus傭兵スパイウェアのエクスプロイトで、携帯電話の広範な制御を取得することに関与していました。

相互運用性要求の詳細について

- DMAの下で初めて公表されたこの要求において、アプリケーションプログラミングインターフェース（API、ソフトウェアプログラムが相互に要求と応答を通信する方法）にアクセスできるようにすることをデベロッパーは求めていますが、これにはLinuxエミュレーターアプリが桁違いの速度や効率で命令を実行できるように、また、バッテリー寿命を延ばすために電力消費を抑えられるようにするといった狙いがあります。これらは、DMA相互運用性規則が実現しようとしている主なメリットでもあります。
- Appleは、DMAの別の箇所に準拠するためにJITを有効化するAPIを構築し、信頼できるブラウザデベロッパーが、独自のJITエンジンを搭載した独自のWebブラウザを提供できるようにしました。しかし、DMAの下では、デベロッパーはApple独自のJITエンジンへの平等なアクセスを要求することが認められています。「同一の機能への相互運用性を、平等な条件の下で認めなければならない」と、規則によって広く定められているためです。

これが重要である理由

- デベロッパーは、DMAの下で説明されている手順に従い、DMAの規則が何に対処することを目的としているのかの把握に努めていますが、DMAの規則に内在する不安を露にしています。しかし、AppleにJITの直接読み取り/書き込み/実行アクセスを誰もが利用できるように強制すると、iPhoneユーザーのセキュリティに対する計算が根本的に変わってしまう可能性があります。
- もしAppleが、この機能をどの開発者にも開放することを強制された場合、前例のない新たなセキュリティリスクが生じ、国家レベルの攻撃者に有利に働き、企業の中核的な業務運用の完全性が危険にさらされるということになりかねません。
- これにより、重大なサイバーリスクが職場でモバイルプラットフォームを活用している欧州の組織の82%にまで拡大する可能性があります。
- DMAの執行者は、これらの相互運用性に関する命令を再考し、その要件が意図せずユーザーをより大きなセキュリティリスクにさらすことのないようにすべきです。またこれは、DMAと同種の政策の再現を目論むあらゆる政策立案者にとっての重大な警戒信号でもあります。

→ 詳しくはこちら。