TRUSTED FUTURE

JIT 사태

DMA의 첫 상호운용성 요청 살펴보기

➔ 기초적인 적시 컴파일 기능에 무제한으로 액세스하거나 안전하지 않은 JIT를 사용하면 해커가 쉽게 악용할 수 있는 심각한 취약점이 발생할 수 있습니다.

유럽연합(EU)이 디지털 시장법(Digital Markets Act, DMA)을 시행했지만, 해당 법에 따른 의무는 가혹한 기술적 현실을 마주하고 있습니다. 게다가 디지털 시장법에 의한 규제 중 일부는 사실은 사이버 보안을 약화시키고 있습니다. Trusted Future의 짐 콜렌버거(Jim Kohlenberger)가 작성한 새로운 브리핑에서는 상호운용성 요청이 어떻게 심각한 보안 취약성을 노출하고 있는지 살펴보고, DMA 집행 기관은 이러한 요청으로 인해 사용자가 의도치 않게 더 높은 보안 위험에 노출되는 일이 없도록 할 것을 촉구합니다.

무슨 일이 일어난 건가요?

- EU의 디지털 시장법에 따르면 대형 디지털 기업, 즉 '게이트키퍼'로 확인된 기업은 자사의 소프트웨어 및 하드웨어가 서드파티 개발자와 상호 운용될 수 있도록 해야 합니다.
- 개발자가 공적으로 게시한 첫 번째 상호 운용성 요청은 Apple에 적시 컴파일러 또는 JIT 엔진의 기능에 직접 액세스할 수 있도록 해달라는 것이었습니다.
- 이 사례는 EU의 경쟁 규제가 실제 상황에서 사이버 보안에 실제로 어떤 영향을 미치는지 평가할 수 있는 첫 번째 기회가 되었습니다.

상호 운용성이 중요한 이유는 무엇인가요?

- 디지털 세계에서 상호운용성은 소비자와 기업에게 엄청난 이점을 가져다 줄 수 있습니다.
- 스마트폰에 내장된 상호운용성 툴은 수백만 개의 서드파티 앱이 디바이스에 탑재된 센서, 컴퓨팅 성능 및 연결 서비스를 연동하며 서드파티 연결 앱 및 디바이스의 에코시스템을 활성화하는 데 도움이 되었습니다.
- 지금까지 이러한 상호운용성은 모든 사용자의 안전, 보안 및 개인 정보를 보호하기 위한 안전장치가 내장되어 있었으며, 이에 따라 광범위한 경제적 이익을 창출했습니다.
- 그러나 의무화된 상호운용성은 이러한 안전장치를 해치거나 약화시킵니다. 게다가 소비자의 기본적인 개인정보, 안전 및 보안을 위험에 빠뜨리는 방식으로 이루어질 경우 문제가 될 수 있습니다.

JIT란 무엇인가요?

- 적시 컴파일러 또는 JIT(Just-In-Time) 엔진은 웹 브라우저가 웹 기반 언어에서 스마트폰의 운영 체제가 이해하는 언어로 코드를 컴파일하는 데 사용하는 소프트웨어입니다. 웹 브라우저가 빠르고 효율적으로 작동하는 데 필요한 요소이자 빠질 수 없는 기능입니다. 또한 매우 복잡하기도 합니다.
- JIT는 최신 브라우저에서 사용하는 기초적인 기술로, 사용자가 게임, Gmail, Instagram, TikTok 등 수백만 개의 복잡한 인터랙티브 웹사이트에 더 빠르고 효율적이며 원활하게 액세스할 수 있도록 해줍니다.
- JIT 기능은 웹페이지에서 텍스트 기반 JavaScript 코드를 가져온 뒤, 일련의 복잡한 파이프라인을 통해 운영 체제에서 더 빠르게 실행할 수 있는 더 효율적인 머신 코드로 컴파일하거나 번역하는 작업을 거칩니다. 이로써 복잡한 웹사이트를 훨씬 더 효율적으로 실행할 수 있게 됩니다.
- 현재 모든 주요 브라우저는 이러한 JIT 엔진을 사용하고 있으며, 이 엔진을 사용하면 상당히 인상적인 성능 향상을 달성할 수 있습니다. 하지만 이러한 성능 향상에는 보안 위험이 수반됩니다: 이러한 인상적인 이점을 실현하는 데

도움이 되는 핵심 기능 중 하나가 바로 JIT 엔진이 메모리의 쓰기 권한을 가지며, 나중에 해당 메모리를 코드로 실행할 수 있다는 점입니다.

- 해커들이 JIT 엔진을 주요 표적으로 삼는 이유는 다음과 같습니다.
  - 브라우저 취약점 공격의 약 절반을 차지함
  - 디버깅이 어려움
  - 임의 코드 실행으로 이어질 수 있음
  - 매우 유해하고 극단적인 취약점 공격이 있음
- 우리는 이미 현실에서 어떤 결과가 일어났는지 알고 있습니다. JIT는 스마트폰의 읽기/쓰기/실행 부분에 멀웨어를 메인라인으로 침투시키는 정교한 연결고리의 일부가 되어, 오리지널 페가수스(Pegasus) 용병 스파이웨어 취약점 공격에서 스마트폰의 광범위한 제어권을 획득하는 데 관여했습니다.

상호운용성 요청의 세부 내용은 무엇인가요?

- DMA에 따라 최초로 공시된 이 요청에서 개발자는 애플리케이션 프로그래밍 인터페이스(Application Programming Interface, API, 소프트웨어 프로그램이 서로 요청과 응답을 주고받는 방식)에 대한 액세스를 요청했습니다. 이 요청을 한 이유는 Linux 에뮬레이터 앱을 훨씬 더 빠르고 효율적으로 실행하여, 나아가 전력 소모량을 줄여 배터리 수명을 연장하기 위함이었습니다. 이는 DMA 상호운용성 규칙이 의도하는 주요 이점 중 하나입니다.
- Apple은 신뢰할 수 있는 브라우저 개발자가 자체 JIT 엔진으로 자체 웹 브라우저를 제공할 수 있도록 DMA의 다른 부분을 준수하는 JIT 지원 API를 구축했습니다. 그러나 DMA에 따르면 '상호운영성은 동일한 기능에 대해 동등한 조건에서 부여되어야 한다'는 규정이 광범위하게 적용되어야 하므로, 요청을 한 개발자는 Apple의 자체 JIT 엔진에 대해 동등한 접근 권한을 요청할 수 있습니다.

이 사항이 왜 중요한가요?

- 개발자가 DMA에 명시된 단계를 따르고, DMA의 규정이 해결하도록 설계된 사항을 추구하고 있지만, 이러한 행동은 DMA 규정에 내재된 긴장감을 드러내고 있습니다. 그러나 Apple로 하여금 JIT의 직접 읽기/쓰기/실행 액세스 권한을 모든 사용자에게 개방하도록 강제할 경우, iPhone 사용자들의 보안 계산법이 근본적으로 바뀔 수 있습니다.
- Apple이 이 기능을 모든 개발자에게 개방하도록 강요한다면 전례 없는 새로운 보안 위험이 발생하고, 국가 차원의 위협 행위자들이 유리한 고지를 점하게 되며, 핵심 기업 비즈니스 운영의 무결성이 위험에 처할 수 있습니다.
- 이렇게 된다면 직장에서 모바일 플랫폼을 활용하는 82%의 유럽 조직에 심각한 사이버 위험에 노출될 가능성이 늘어날 수도 있습니다.
- DMA 집행 기관은 이러한 상호운용성 의무를 재고하고, 해당 요청으로 인하여 사용자가 의도치 않게 더 높은 보안 위험에 노출되는 일이 없도록 해야 합니다. 그리고 이는 DMA와 유사한 정책을 모방하려는 모든 정책 입안자에게 보내는 위험 신호입니다

→ 여기에서 자세히 알아보세요.