

MẶT TRÁI CỦA JIT

GÓC NHÌN VỀ YÊU CẦU TƯƠNG TÁC ĐẦU TIÊN THEO ĐẠO LUẬT DMA

➔ Khả năng truy cập không giới hạn vào các tính năng biên dịch Just-In-Time (JIT) nền tảng hay việc sử dụng JIT không an toàn tạo ra những lỗ hổng nghiêm trọng mà tin tặc có thể dễ dàng lợi dụng.

Khi Liên minh Châu Âu (EU) triển khai Đạo luật Thị trường kỹ thuật số (DMA), những quy định liên quan đã vấp phải thực tế khắc nghiệt trên phương diện kỹ thuật: một số quy định thực chất lại đang làm suy yếu an ninh mạng. [Trong bài phân tích mới](#) của mình, Jim Kohlenberger đến từ Trusted Future sẽ chỉ ra những lỗ hổng bảo mật nghiêm trọng mà yêu cầu về khả năng tương tác gây ra, đồng thời kêu gọi các cơ quan thực thi DMA đảm bảo yêu cầu của đạo luật này không vô tình làm tăng rủi ro bảo mật đối với người dùng.

ĐIỀU GÌ ĐÃ XẢY RA?

- Đạo luật Thị trường kỹ thuật số do EU ban hành yêu cầu các công ty kỹ thuật số lớn – tức những công ty được xem là “đơn vị kiểm soát” hệ sinh thái – phải đảm bảo phần mềm và phần cứng của họ tương tác được với nhà phát triển bên thứ ba.
- Yêu cầu tương tác đầu tiên do một nhà phát triển gửi công khai đã yêu cầu Apple cung cấp quyền truy cập trực tiếp vào các tính năng trong Trình biên dịch Just-In-Time (hay còn gọi là bộ xử lý JIT) của Apple.
- Đây là cơ hội đầu tiên để chúng ta đánh giá xem các quy định cạnh tranh của EU thực sự ảnh hưởng đến an ninh mạng như thế nào trong bối cảnh thực tế.

TẠI SAO KHẢ NĂNG TƯƠNG TÁC LẠI QUAN TRỌNG?

- Trong thế giới số, khả năng tương tác đem lại lợi ích to lớn cho cả người tiêu dùng và doanh nghiệp.
- Nhờ các công cụ tương tác tích hợp trong điện thoại thông minh, hàng triệu ứng dụng bên thứ ba có thể hoạt động với cảm biến trên bo mạch, năng lực xử lý và dịch vụ kết nối trên thiết bị, qua đó hình thành nên hệ sinh thái ứng dụng và thiết bị kết nối của bên thứ ba.
- Cho đến nay, khả năng tương tác đã tạo ra lợi ích kinh tế trên diện rộng, một phần nhờ tích hợp sẵn các cơ chế bảo vệ để nâng cao tính an toàn, bảo mật và quyền riêng tư của mọi người dùng.
- Tuy nhiên, khi trở thành yêu cầu bắt buộc, khả năng tương tác có thể gây ra vấn đề nếu cách thực thi gây hại hoặc làm giảm khả năng bảo vệ của những cơ chế này, từ đó gây rủi ro cho quyền riêng tư, sự an toàn và bảo mật căn bản của người dùng.

JIT LÀ GÌ?

- Trình biên dịch Just-In-Time hay bộ xử lý JIT là phần mềm mà các trình duyệt web sử dụng để biên dịch mã lệnh từ ngôn ngữ web sang ngôn ngữ mà hệ điều hành của điện thoại thông minh hiểu được. Đây là một chức năng quan trọng, cần thiết và không thể thiếu để trình duyệt web có thể hoạt động nhanh chóng và hiệu quả. Tuy nhiên, công nghệ này cũng cực kỳ phức tạp.

- JIT là kỹ thuật nền tảng được dùng trong các trình duyệt hiện đại, giúp người dùng truy cập những trang web tương tác phức tạp như trò chơi, Gmail, Instagram, TikTok, cũng như hỗ trợ hàng triệu trang web khác chạy nhanh hơn, hiệu quả hơn và mượt mà hơn.
- Với chức năng JIT, các trang web phức tạp này có thể nâng cao đáng kể hiệu suất hoạt động bằng cách biên dịch mã JavaScript dạng văn bản trên trang web qua một chuỗi quy trình phức tạp để có được mã máy tối ưu hơn, chạy nhanh hơn trong hệ điều hành.
- Các bộ xử lý JIT như vậy hiện được dùng trong mọi trình duyệt lớn và có thể mang lại hiệu suất ấn tượng. Tuy nhiên, lợi ích hiệu suất đó đi kèm với rủi ro cao hơn về bảo mật: một trong những tính năng chính giúp đạt được hiệu suất ấn tượng như vậy là bộ xử lý JIT được phép vừa ghi dữ liệu vào bộ nhớ, vừa thực thi chính bộ nhớ đó như mã lệnh.
- Các bộ xử lý JIT đã trở thành mục tiêu chính của tin tặc vì:
 - Gây ra một nửa số vụ khai thác lỗ hổng trình duyệt
 - Khó gỡ lỗi
 - Có thể dẫn đến thực thi mã tùy ý
 - Có những lỗ hổng rất nguy hiểm và nghiêm trọng
- Chúng ta đều đã biết hậu quả thực tế: Trong vụ khai thác lỗ hổng bảo mật [trên bản gốc của phần mềm gián điệp cho thuê Pegasus](#), JIT từng là một mắt xích trong chuỗi tấn công tinh vi với mục tiêu cài mã độc vào vùng bộ nhớ đọc/ghi/thực thi của điện thoại thông minh nhằm chiếm quyền kiểm soát điện thoại.

YÊU CẦU TƯƠNG TÁC CÓ NỘI DUNG NHƯ THẾ NÀO?

- Trong yêu cầu đầu tiên theo quy định DMA, một [nhà phát triển](#) đề nghị được cấp quyền truy cập vào giao diện lập trình ứng dụng (gọi tắt là API – công cụ hỗ trợ các chương trình phần mềm trao đổi yêu cầu và phản hồi với nhau) để giúp ứng dụng giả lập Linux của họ chạy nhanh hơn và hiệu quả hơn gấp nhiều lần, đồng thời sử dụng ít năng lượng hơn nhằm tăng thời lượng pin. Nói cách khác, họ muốn đạt được những lợi ích chính mà DMA hướng tới thông qua quy định về khả năng tương tác.
- Apple đã xây dựng [API hỗ trợ JIT](#) để tuân thủ một quy định khác của DMA, đó là cho phép các nhà phát triển trình duyệt đáng tin cậy chạy trình duyệt web bằng bộ xử lý JIT của riêng họ. Tuy nhiên, DMA còn cho phép nhà phát triển yêu cầu quyền truy cập bình đẳng vào bộ xử lý JIT của chính Apple, vì quy định của đạo luật này bao quát rằng [“khả năng tương tác phải được cấp cho cùng một tính năng với cùng điều kiện”](#).

TẠI SAO VẤN ĐỀ NÀY LẠI QUAN TRỌNG?

- Mặc dù nhà phát triển này tuân theo các bước mà DMA đề ra và cho rằng mình đang yêu cầu đúng mục tiêu của đạo luật, nhưng điều này làm lộ rõ mâu thuẫn nội tại trong chính quy định của DMA. Việc buộc Apple phải cấp cho bất kỳ ai quyền đọc/ghi/thực thi trực tiếp của JIT có thể làm thay đổi căn bản cấu trúc bảo mật đối với người dùng iPhone.
- Nếu Apple buộc phải cấp tính năng này cho mọi nhà phát triển, điều đó có thể dẫn đến những lỗ hổng chưa từng có tiền lệ, tạo điều kiện cho các tác nhân đe dọa an ninh quốc gia và gây rủi ro cho tính toàn vẹn của hoạt động kinh doanh cốt lõi.
- Việc này có thể làm tăng đáng kể rủi ro an ninh mạng đối với [82% các tổ chức châu Âu đang sử dụng nền tảng di động](#) trong công việc.
- Các cơ quan thực thi DMA nên cân nhắc lại những quy định về khả năng tương tác và đảm bảo yêu cầu của đạo luật này không vô tình khiến người dùng đối mặt với rủi ro bảo mật cao hơn. Đây cũng là hồi chuông cảnh báo cho bất kỳ nhà hoạch định chính sách nào muốn đặt ra quy định tương tự như DMA.

➔ **ĐỌC THÊM [TẠI ĐÂY](#).**