CÔNG AN TỈNH ĐỒNG NAI

BẢN TIN
AN NINH MẠNG

TUẦN 1 • THÁNG 12/2025

PHÒNG AN NINH MẠNG VÀ PHÒNG, CHỐNG TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO

02513.685.134

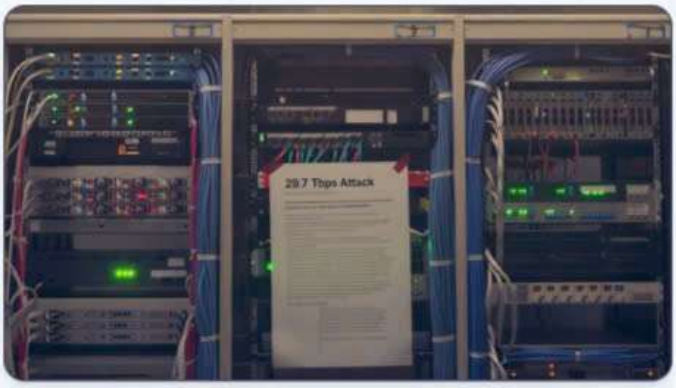
attt@dongnai.gov.vn

MÃ ĐỘC

MẠNG BOT AISURU TẤN CÔNG TỪ CHỐI DỊCH VỤ QUY MÔ LỚN ĐẠT KỶ LỤC 29.7 TBPS

> ***"Cuộc tấn công DDoS kỷ lục này nhấn mạnh sự cần thiết phải tăng cường bảo mật và khả năng phòng thủ trước các mối đe dọa mạng ngày càng tinh vi."***

Cloudflare vừa công bố đã phát hiện và giảm thiểu một cuộc tấn công từ chối dịch vụ phân tán (DDoS) lớn nhất từ trước đến nay, đạt mức 29.7 terabit mỗi giây (Tbps). Cuộc tấn công này được cho là có nguồn gốc từ mạng bot AISURU, một dịch vụ botnet cho thuê khét tiếng, vốn đã thực hiện nhiều cuộc tấn công DDoS với lưu lượng cực lớn trong năm qua. Cuộc tấn công kéo dài 69 phút, gây gián đoạn đáng kể cho các dịch vụ trực tuyến.



(Hình ảnh minh họa)

Mạng bot AISURU, với ước tính lên đến 4 triệu máy chủ bị nhiễm, cho phép tin tặc thực hiện các cuộc tấn công DDoS với quy mô chưa từng thấy. Việc khai thác các lỗ hổng bảo mật và sử dụng các kỹ thuật khuếch đại lưu lượng truy cập đã giúp AISURU tạo ra lượng dữ liệu khổng lồ, làm quá tải các hệ thống mục tiêu và gây ra tình trạng từ chối dịch vụ. Sự việc này gióng lên hồi chuông cảnh báo về sự gia tăng của các cuộc tấn công DDoS phức tạp và nguy hiểm.

NGUỒN TIN
The Hacker News

LIÊN KẾT GỐC
https://thehackernews.com/2025/12/record-297-tbps-ddos-attack-linked-to.html

Bản tin được tổng hợp tự động. Vui lòng tham khảo thông tin chi tiết tại đường dẫn gốc.

MÃ ĐỘC

GOLDFACTORY TẤN CÔNG ĐÔNG NAM Á QUA ỨNG DỤNG NGÂN HÀNG GIẢ MẠO GÂY RA HƠN 11000 CA NHIỄM

> ***"Người dùng cần đặc biệt cảnh giác với các ứng dụng ngân hàng không rõ nguồn gốc để tránh trở thành nạn nhân của GoldFactory."***

Nhóm tội phạm mạng GoldFactory đang thực hiện các cuộc tấn công mới nhằm vào người dùng di động ở Indonesia, Thái Lan và Việt Nam bằng cách mạo danh các dịch vụ chính phủ. Hoạt động này, được ghi nhận từ tháng 10 năm 2024, liên quan đến việc phát tán các ứng dụng ngân hàng đã được sửa đổi, đóng vai trò như một kênh dẫn cho phần mềm độc hại Android. Các ứng dụng giả mạo này được thiết kế để lừa người dùng cài đặt chúng, từ đó tạo điều kiện cho kẻ tấn công xâm nhập và kiểm soát thiết bị.

(Hình ảnh minh họa)

GoldFactory sử dụng các ứng dụng ngân hàng đã bị can thiệp để phát tán mã độc. Khi người dùng cài đặt ứng dụng giả mạo, phần mềm độc hại sẽ âm thầm hoạt động, đánh cắp thông tin tài chính nhạy cảm, thông tin cá nhân và thậm chí kiểm soát thiết bị từ xa. Số lượng lớn các ca nhiễm cho thấy quy mô và mức độ nguy hiểm của chiến dịch tấn công này, gây ra rủi ro tài chính nghiêm trọng cho người dùng ở khu vực Đông Nam Á.

NGUỒN TIN
The Hacker News

LIÊN KẾT GỐC
https://thehackernews.com/2025/12/goldfactory-hits-southeast-asia-with.html

Bản tin được tổng hợp tự động. Vui lòng tham khảo thông tin chi tiết tại đường dẫn gốc.

LỖ HỔNG BẢO MẬT

TIN TẶC CÓ THỂ THỰC THI MÃ TỪ XA QUA LỖ HỔNG NGHIÊM TRỌNG TRONG REACT SERVER COMPONENTS VÀ NEXT.JS

> ***"Lỗ hổng RCE nghiêm trọng đe dọa các ứng dụng React và Next.js. Cần cập nhật ngay lập tức để ngăn chặn các cuộc tấn công tiềm ẩn."***

Các lỗ hổng nghiêm trọng được phát hiện trong giao thức Flight được sử dụng bởi React Server Components và Next.js, cho phép tin tặc thực thi mã từ xa (RCE) với điểm CVSS đạt mức cao nhất là 10.0. Các lỗ hổng này được theo dõi dưới dạng CVE-2025-55182 và CVE-2025-55182-66478, gây ra rủi ro đặc biệt nguy hiểm cho các ứng dụng web sử dụng các công nghệ này. Việc khai thác thành công có thể cho phép kẻ tấn công chiếm quyền kiểm soát hoàn toàn máy chủ.

(Hình ảnh minh họa)

Cụ thể, lỗ hổng nằm trong quá trình xử lý dữ liệu không đáng tin cậy được truyền qua giao thức Flight. Kẻ tấn công có thể lợi dụng điều này để chèn mã độc vào máy chủ, từ đó thực thi các lệnh tùy ý. Điều này có thể dẫn đến việc đánh cắp dữ liệu nhạy cảm, cài đặt phần mềm độc hại hoặc thậm chí làm gián đoạn hoàn toàn hoạt động của ứng dụng. Các nhà phát triển nên khẩn trương áp dụng các biện pháp bảo mật cần thiết.

NGUỒN TIN
Unit 42

LIÊN KẾT GỐC
https://unit42.paloaltonetworks.com/cve-2025-55182-react-and-cve-2025-66478-next/

Bản tin được tổng hợp tự động. Vui lòng tham khảo thông tin chi tiết tại đường dẫn gốc.

LỖ HỔNG BẢO MẬT

KHAI THÁC LỖ HỔNG NGHIÊM TRỌNG TRONG YETH CHO PHÉP TIN TẶC ĐÁNH CẮP 9 TRIỆU ĐÔ LA

> ***"Lỗ hổng yETH phơi bày điểm yếu DeFi, cần tăng cường bảo mật và kiểm tra để bảo vệ tài sản người dùng."***

Một lỗ hổng đặc biệt nghiêm trọng trong giao thức tài chính phi tập trung (DeFi) yETH đã bị khai thác thành công, dẫn đến việc tin tặc chiếm đoạt số tiền trị giá 9 triệu đô la Mỹ. Lỗ hổng này cho phép kẻ tấn công thực hiện các giao dịch trái phép và rút tiền từ các hợp đồng thông minh của yETH mà không cần xác thực. Vụ việc nhấn mạnh những rủi ro tiềm ẩn liên quan đến các giao thức DeFi và sự cần thiết phải có các biện pháp bảo mật mạnh mẽ để bảo vệ tài sản của người dùng.

(Hình ảnh minh họa)

Việc khai thác này cho thấy tin tặc liên tục tìm kiếm và khai thác các lỗ hổng trong các ứng dụng blockchain và DeFi. Hậu quả của vụ việc này có thể gây ảnh hưởng nghiêm trọng đến niềm tin của nhà đầu tư vào thị trường DeFi và thúc đẩy các nhà phát triển phải tăng cường kiểm tra bảo mật và các biện pháp phòng ngừa rủi ro. Các tổ chức và cá nhân tham gia vào không gian DeFi nên xem xét kỹ lưỡng các rủi ro liên quan và thực hiện các bước để giảm thiểu những rủi ro đó.

NGUỒN TIN
The Hacker News

LIÊN KẾT GỐC
https://thehackernews.com/2025/12/threatsday-bulletin-wi-fi-hack-npm-worm.html

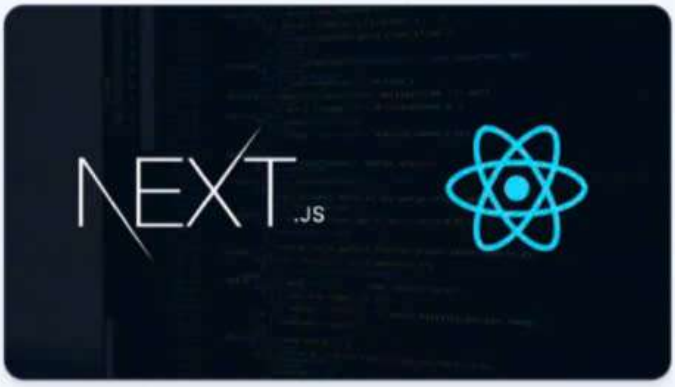
Bản tin được tổng hợp tự động. Vui lòng tham khảo thông tin chi tiết tại đường dẫn gốc.

LỖ HỔNG BẢO MẬT

LỖ HỔNG REACT VÀ NEXT.JS CHO PHÉP THỰC THI MÃ TỪ XA KHÔNG YÊU CẦU XÁC THỰC

> ***"Cập nhật ngay lập tức React và Next.js để ngăn chặn nguy cơ bị khai thác lỗ hổng thực thi mã từ xa."***

Một lỗ hổng bảo mật nghiêm trọng đã được phát hiện trong React Server Components (RSC), có khả năng dẫn đến thực thi mã từ xa nếu bị khai thác thành công. Lỗ hổng này ảnh hưởng đến cách React giải mã các payload được gửi đến React, cho phép tin tặc thực thi mã tùy ý trên hệ thống mục tiêu mà không cần xác thực. Lỗ hổng này đặc biệt nguy hiểm do mức độ nghiêm trọng cao và khả năng bị khai thác dễ dàng.



(Hình ảnh minh họa)

Được theo dõi với mã định danh CVE-2025-55182, lỗ hổng này đạt điểm CVSS tối đa là 10.0. Kẻ tấn công có thể lợi dụng lỗ hổng này để cài đặt phần mềm độc hại, truy cập dữ liệu nhạy cảm hoặc kiểm soát hoàn toàn hệ thống bị ảnh hưởng. Các tổ chức và nhà phát triển sử dụng React và Next.js nên khẩn trương áp dụng các biện pháp giảm thiểu rủi ro được khuyến nghị để bảo vệ khỏi các cuộc tấn công tiềm ẩn.

NGUỒN TIN
The Hacker News

LIÊN KẾT GỐC
https://thehackernews.com/2025/12/critical-rsc-bugs-in-react-and-nextjs.html

Bản tin được tổng hợp tự động. Vui lòng tham khảo thông tin chi tiết tại đường dẫn gốc.

LỖ HỔNG BẢO MẬT

TIN TẶC TẬN DỤNG LỖ HỔNG KING ADDONS ĐỂ TẠO TÀI KHOẢN QUẢN TRỊ TRÊN WORDPRESS

> ***"Cập nhật plugin King Addons ngay lập tức để ngăn chặn tin tặc chiếm quyền kiểm soát trang web WordPress của bạn."***

Một lỗ hổng bảo mật nghiêm trọng ảnh hưởng đến plugin WordPress có tên King Addons cho Elementor đang bị khai thác tích cực trên thực tế. Lỗ hổng CVE-2025-8489 (điểm CVSS: 9.8) là một trường hợp leo thang đặc quyền, cho phép những kẻ tấn công không yêu cầu xác thực cấp cho chính họ các đặc quyền quản trị bằng cách chỉ định vai trò người dùng quản trị viên trong quá trình đăng ký. Điều này có nghĩa là tin tặc có thể tạo tài khoản quản trị mới mà không cần bất kỳ thông tin đăng nhập hợp lệ nào.

(Hình ảnh minh họa)

Việc khai thác thành công lỗ hổng cho phép tin tặc kiểm soát hoàn toàn trang web WordPress bị ảnh hưởng. Kẻ tấn công có thể tùy ý cài đặt phần mềm độc hại, sửa đổi nội dung trang web, đánh cắp dữ liệu nhạy cảm và thực hiện nhiều hành động độc hại khác. Các quản trị viên WordPress sử dụng plugin King Addons được khuyến cáo khẩn cấp cập nhật lên phiên bản mới nhất để ngăn chặn việc khai thác lỗ hổng này.

NGUỒN TIN
The Hacker News

LIÊN KẾT GỐC
https://thehackernews.com/2025/12/wordpress-king-addons-flaw-under-active.html

Bản tin được tổng hợp tự động. Vui lòng tham khảo thông tin chi tiết tại đường dẫn gốc.

LUẬT & CHÍNH SÁCH

PHÂN TÍCH PHẦN MỀM ĐỘC HẠI BRICKSTORM SỬ DỤNG CHO DUY TRÌ TRUY CẬP TRÁI PHÉP

> ***"Các tổ chức nên sử dụng các chỉ số thỏa hiệp (IOC) và chữ ký phát hiện để xác định các mẫu phần mềm độc hại BRICKSTORM."***

Cơ quan An ninh mạng và Cơ sở hạ tầng (CISA), Cơ quan An ninh Quốc gia (NSA) và Trung tâm An ninh Mạng Canada (Cyber Centre) đã đánh giá rằng các tin tặc được nhà nước Cộng hòa Nhân dân Trung Hoa (PRC) bảo trợ đang sử dụng phần mềm độc hại BRICKSTORM để duy trì truy cập trái phép lâu dài trên các hệ thống bị xâm nhập, chủ yếu nhắm vào các tổ chức trong lĩnh vực dịch vụ chính phủ, cơ sở hạ tầng và công nghệ thông tin. BRICKSTORM là một backdoor phức tạp được thiết kế cho VMware vSphere và môi trường Windows. Sau khi xâm nhập, tin tặc có thể sử dụng quyền truy cập vào bảng điều khiển quản lý vCenter để đánh cắp các bản sao ảo của máy ảo (VM) cho mục đích trích xuất thông tin đăng nhập và tạo các VM ẩn, giả mạo.

(Hình ảnh minh họa)

BRICKSTORM hoạt động bằng cách chạy các kiểm tra và duy trì sự bền bỉ bằng cách sử dụng chức năng tự theo dõi. Nó sử dụng nhiều lớp mã hóa (HTTPS, WebSockets, TLS lồng nhau) để che giấu liên lạc với máy chủ C2 của tin tặc. Ngoài ra, nó sử dụng DNS-over-HTTPS (DoH) và bắt chước chức năng của máy chủ web để hòa trộn liên lạc của nó với lưu lượng truy cập hợp pháp. BRICKSTORM cung cấp cho tin tặc khả năng truy cập shell tương tác trên hệ thống, cho phép họ duyệt, tải lên, tải xuống, tạo, xóa và thao tác các tệp. Một số mẫu còn hoạt động như một proxy SOCKS, tạo điều kiện cho việc di chuyển ngang và cho phép tin tặc xâm nhập vào các hệ thống khác.

NGUỒN TIN
All CISA Advisories

LIÊN KẾT GỐC
https://www.cisa.gov/news-events/analysis-reports/ar25-338a

Bản tin được tổng hợp tự động. Vui lòng tham khảo thông tin chi tiết tại đường dẫn gốc.