BỘ CÔNG AN
CÔNG AN TỈNH QUẢNG NGÃI

Số: 150 /CAT-ANM

V/v cảnh báo lỗ hổng bảo mật nghiêm trọng tháng 6/2025

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Quảng Ngãi, ngày 03 tháng 7 năm 2025

Kính gửi:
- Ủy ban MTTQ Việt Nam tỉnh;
- Văn phòng Tỉnh ủy, UBND tỉnh;
- Văn phòng Đoàn ĐBQH&HĐND tỉnh;
- Các sở, ban, ngành; Hội, đoàn thể tỉnh;
- UBND các xã, phường, Đặc khu Lý Sơn;
- Trường Đại học Phạm Văn Đồng;
- Trường Cao đẳng Cộng đồng Kon Tum;
Cao đẳng Việt Nam - Hàn Quốc - Quảng Ngãi;
- Điện lực Quảng Ngãi; Công ty CP Lọc hóa dầu Bình Sơn; Truyền tải điện Quảng Ngãi.

Trong tháng 6/2025, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an đã thực hiện phân tích và tổng hợp đối với **10** lỗ hổng bảo mật nghiêm trọng ảnh hưởng đến hệ thống thông tin của Việt Nam *(Tài liệu lưu hành nội bộ)*. Trong đó, có 04 lỗ hổng bảo mật có mức độ rất nghiêm trọng, 04 lỗ hổng bảo mật nghiêm trọng, 02 lỗ hổng bảo mật mức trung bình (trong đó 02 lỗ hổng đã công khai POC), cụ thể:

1. Lỗ hổng bảo mật trên hệ điều hành của Microsoft

*** CVE-2025-32711** - Lỗ hổng AI Zero-Click làm lộ dữ liệu Microsoft 365 Copilot

- Mô tả:

+ Điểm CVSS: 9.3/10; Mức độ: Critical.

+ Đầu tiên, kẻ tấn công có thể gửi một email hoặc tài liệu định dạng đơn giản như văn bản markdown đến hộp thư Outlook của nạn nhân, bên trong chứa một đoạn prompt injection được ngụy trang tinh vi. Dù người dùng không mở email, nội dung này vẫn tồn tại trong không gian dữ liệu có thể truy xuất bởi Microsoft 365 Copilot để phục vụ các tác vụ phân tích hoặc tạo nội dung. Tiếp theo, đoạn mã độc được ngụy trang như một chỉ dẫn hội thoại tự nhiên thông thường, khiến cho mô hình ngôn ngữ hiểu sai là yêu cầu hợp lệ, từ đó dễ dàng vượt qua bộ lọc kiểm soát prompt injection - XPIA của Microsoft mà không bị phát hiện. Sau đó, khi người dùng đặt câu hỏi cho Microsoft 365 Copilot, hệ thống sẽ kích hoạt cơ chế Retrieval-Augmented Generation (RAG) để tự động tìm kiếm và tổng hợp thông tin liên quan từ nhiều nguồn nội bộ như Outlook, SharePoint hoặc Teams. Lúc này, đoạn lệnh ngầm được kích hoạt, âm thầm

"đánh lừa" mô hình ngôn ngữ (LLM), khiến Copilot hiểu nhầm chỉ thị từ kẻ tấn công là yêu cầu hợp lệ và thực thi prompt được nhúng sẵn.

- Phiên bản ảnh hưởng: Tất cả hệ điều hành Windows sử dụng phần mềm Microsoft 365 Copilot.

- Khuyến nghị: Microsoft đã xác nhận trong thông báo tương ứng của mình rằng sự cố đã được giải quyết hoàn toàn và khách hàng không cần thực hiện thêm hành động nào nữa. Microsoft cung cấp các thẻ DLP để chặn xử lý email bên ngoài, cùng với tính năng M365 Roadmap mới hạn chế Copilot truy cập vào các email được gắn nhãn bằng thẻ nhạy cảm: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025- 32711.

- Lỗ hổng chưa có PoC công khai.

* **CVE-2025-47966** - Lỗ hổng nâng cao đặc quyền của Microsoft Power Automate.

- Mô tả: Điểm CVSS 9.8/10; Mức độ: Critical; Lỗ hổng này trong Power Automate được tin tặc thu thập thông tin nhạy cảm, cho phép leo thang đặc quyền qua mạng. Power Automate là một công cụ của Microsoft để tự động hóa các tác vụ lặp lại và quy trình kinh doanh trên nhiều ứng dụng và dịch vụ khác nhau.

- Phiên bản ảnh hưởng: Tất cả hệ điều hành Windows sử dụng phần mềm Power Automate.

- Khuyến nghị: Microsoft đã báo cáo rằng lỗ hổng này đã được giảm thiểu hoàn toàn và người dùng không cần thực hiện thêm hành động nào nữa: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47966.

- Lỗ hổng chưa có PoC công khai.

2. Lỗ hổng bảo mật phần mềm trên hệ điều hành Linux

* **CVE-2025-38032** - Lỗ hổng ghi ngoài giới hạn trong Linux Kernel.

- Mô tả: Điểm CVSS 7.1/10; Mức độ: High; Lỗ hổng trong hạt nhân Linux do lỗi ghi ngoài giới hạn. Nếu tin tặc viết nhiều ký tự hơn, số lượng sẽ không bị cắt bớt đến không gian khả dụng tối đa trong "simple_write_to_buffer" mà vượt quá kích thước đầu vào so với kích thước bộ đệm.

- Phiên bản ảnh hưởng: Các phiên bản kali linux từ 6.13 đến trước 6.15.

- Khuyến nghị: Các bản phân phối Linux đã ban hành khuyến cáo bảo mật, với các bản vá hiện có sẵn cho tất cả các nhánh được bảo trì. Điều cần thiết là người dùng phải kiểm tra phiên bản đang sử dụng và cập nhật các hệ thống chạy phiên bản mới nhất.

- Lỗ hổng chưa có PoC công khai.

3. Lỗ hổng bảo mật phần mềm trên tường lửa

* **CVE-2025-0130** - Lỗ hổng từ chối dịch vụ (DoS) của tường lửa trong tính năng Web-Proxy.

- Mô tả: Điểm CVSS 8.2/10; Mức độ: High; Lỗ hổng xảy ra khi kiểm tra ngoại lệ bị thiếu trong phần mềm Palo Alto Networks PAN-OS® với tính năng proxy web được bật cho phép tin tặc chưa xác thực gửi một loạt các gói tin được tạo độc hại khiến tường lửa không phản hồi và cuối cùng khởi động lại.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến PAN-OS 11.0 và các phiên bản PAN-OS mới hơn. Phần mềm PAN-OS 11.0 đã hết vòng đời (EoL) sẽ không được khắc phục sự cố này trong phiên bản này.

- Khuyến nghị: Sự cố này chỉ ảnh hưởng đến tường lửa PAN-OS có bật tính năng proxy web. Nhà phát hành khuyến nghị tắt tính năng proxy web nếu không sử dụng để giảm thiểu sự cố này. Để biết thêm thông tin chi tiết: https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-new-features/networking-features/web-proxy.

- Lỗ hổng chưa có PoC công khai.

4. Lỗ hổng bảo mật phần mềm trên dịch vụ Web

*** CVE-2025-47577** - Lỗ hổng trong plugin TI WooCommerce Wishlist trên trang Web WordPress.

- Mô tả: Điểm CVSS 10/10; Mức độ: Critical; Lỗ hổng này cho phép tin tặc tải lên các tệp tùy ý, bao gồm cả web Shell, lên máy chủ web bị ảnh hưởng mà không cần xác thực. Điều này có khả năng dẫn đến việc xâm phạm hoàn toàn máy chủ vì nó cho phép thực thi mã độc trên hệ thống mục tiêu.

- Phiên bản ảnh hưởng: Tất cả các phiên bản của plugin bên dưới và bao gồm cả phiên bản 2.9.2.

- Khuyến nghị: Patchstack đã phát hành bản vá ảo để giảm thiểu sự cố bằng cách chặn các cuộc tấn công tiềm ẩn cho đến khi bản sửa lỗi chính thức khả dụng. Quản trị viên trang web được khuyên nên triển khai bản vá ảo ngay lập tức hoặc cân nhắc tạm thời vô hiệu hóa và xóa plugin: https://patchstack.com/database/wordpress/plugin/ti-woocommerce-wishlist/vulnerability/wordpress-ti-woocommerce-wishlist-2-9-2-arbitrary-file-upload-vulnerability?_s_id=cve.

- Lỗ hổng có PoC: https://github.com/Yucaerin/CVE-2025-47577.

5. Lỗ hổng bảo mật phần mềm trên dịch vụ Email

*** CVE-2025-5986** - Lỗ hổng liên kết mailbox trong Mozilla Thunderbird.

- Mô tả: Điểm CVSS 6.5/10; Mức độ: Medium; Lỗ hổng này cho phép các email HTML được tạo thủ công bằng cách sử dụng liên kết mailbox:/// để kích hoạt tải xuống tự động.

- Phiên bản ảnh hưởng: Các phiên bản Mozilla Thunderbird trước 128.11.1 và 139.0.2.

- Khuyến nghị: Mozilla đã giải quyết lỗ hổng này trong Thunderbird phiên bản 128.11.1 và 139.0.2. Người dùng được khuyến cáo nên nâng cấp lên các phiên bản này hoặc các phiên bản mới hơn để bảo vệ khỏi vấn đề bảo mật này: https://www.mozilla.org/en-US/security/advisories/mfsa2025-49/.

- Lỗ hổng chưa có PoC công khai.

6. Lỗ hổng bảo mật phần mềm trên ngôn ngữ lập trình

*** CVE-2025-6087** - Lỗ hổng Server-Side Request Forgery (SSRF) trong Next.js.

- Mô tả: Điểm CVSS: 7.8/10; Mức độ: High; Lỗ hổng bắt nguồn từ một tính năng chưa được triển khai trong bộ điều hợp Cloudflare cho Open Next, cho phép người dùng chưa xác thực ủy quyền nội dung từ xa tùy ý thông qua điểm cuối /_next/image. Sự cố này cho phép tin tặc tải tài nguyên từ xa từ các máy chủ tùy ý dưới tên miền của trang web nạn nhân cho bất kỳ trang web nào được triển khai bằng bộ điều hợp Cloudflare cho Open Next.

- Phiên bản ảnh hưởng: Tất cả các trang web sử dụng Next.js được triển khai bằng bộ điều hợp Cloudflare cho OpenNext trước phiên bản 1.3.0.

- Khuyến nghị:

+ Bản sửa lỗi phía máy chủ: Cloudflare đã triển khai bản cập nhật tự động ở cấp nền tảng, hạn chế /_next/image chỉ tải nội dung hình ảnh thực tế, giảm thiểu sự cố cho tất cả các lần triển khai hiện tại và tương lai.

+ Bản vá cơ sở mã với phiên bản an toàn được phát hành là v1.3.0: https://github.com/opennextjs/opennextjs-cloudflare/releases/tag/%40opennextjs%2Fcloudflare%401.3.0.

+ Cập nhật chuỗi phụ thuộc: Cloudflare cũng đã vá gói create-cloudflare với phiên bản bảo mật được cập nhật và phát hành là V2.49.3: https://www.npmjs.com/package/create-cloudflare/v/2.49.3.

- Lỗ hổng chưa có PoC công khai.

7. Lỗ hổng bảo mật phần mềm trên trình duyệt

*** CVE-2025-5419** - Lỗ hổng Zero-Day mới của Chrome, đọc và ghi ngoài giới hạn trong JavaScript V8 và WebAssembly.

- Mô tả: Điểm CVSS 8.8/10; Mức độ: High; Quyền đọc và ghi ngoài giới hạn trong V8 của Google Chrome trước phiên bản 137.0.7151.68 cho phép kẻ tấn công từ xa có khả năng khai thác lỗi heap thông qua trang HTML được tạo thủ công.

- Phiên bản ảnh hưởng: Lỗ hổng bảo mật này ảnh hưởng đến các phiên bản Google Chrome trước 137.0.7151.68.

- Khuyến nghị: Nhà phát hành khuyến nghị người dùng phải nâng cấp lên phiên bản ổn định mới nhất 137.0.7151.68/.69 cho Windows và Mac và 137.0.7151.68 cho Linux. Thông tin chi tiết tham khảo: https://chromereleases.googleblog.com/2Q25/06/stable-channel-update-for-desktop.html.

- Lỗ hổng chưa có PoC công khai.

8. Lỗ hổng bảo mật chuỗi cung ứng khác

* **CVE-2025-24495** - Lỗ hổng trong Branch Prediction Unit (BPU) Lion Core của CPU Intel.

- Mô tả: Điểm CVSS 6.8/10; Mức độ: Medium; Lỗ hổng cho phép tin tặc vượt qua các biện pháp bảo vệ của Indirect Branch Predictor Barrier (IBPB), bằng cách sử dụng các kỹ thuật đào tạo dự đoán nhánh như được mô tả trong "Training Solo", tin tặc có đặc quyền cục bộ có thể sử dụng cách vượt qua này để đánh cắp dữ liệu nhạy cảm từ hệ thống bị ảnh hưởng, bao gồm từ các máy chủ ảo hóa hoặc các máy khách lân cận trong môi trường ảo hóa.

- Phiên bản ảnh hưởng: Các sản phẩm sử dụng CPU Intel Core Ultra 5, 7, 9.

- Khuyến nghị: Nhà phát hành Intel đang cung cấp các bản cập nhật vi mã để giảm thiểu lỗ hổng này, mọi thông tin về lỗ hổng và yêu cầu về hỗ trợ thông qua: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa- 01322.html.

- Lỗ hổng chưa có PoC công khai.

* **CVE-2025-20260** - Lỗ hổng phần mềm diệt virus ClamAV gây lỗi tràn bộ đệm, từ chối dịch vụ và khả năng thực thi mã.

- Mô tả: Điểm CVSS 9.8/10; Mức độ: Critical; Tin tặc có thể khai thác lỗ hổng này bằng cách gửi tệp PDF được tạo thủ công để ClamAV quét trên thiết bị bị ảnh hưởng. Một khai thác thành công có thể cho phép tin tặc kích hoạt tràn bộ đệm, có khả năng dẫn đến việc chấm dứt quy trình quét ClamAV và tình trạng DoS trên phần mềm bị ảnh hưởng.

- Phiên bản ảnh hưởng: Các phiên bản ClamAV 1.4.3 và 1.0.9. trở về trước.

- Khuyến nghị: Nhà phát hành Cisco đã cung cấp các bán vá, người dùng có thể tải xuống trên trang chủ của ClamAV https://www.clamav.net/downloads hoặc trên trang phát hành GitHub https://github.com/Cisco-Talos/clamav/releases hoặc thông qua Docker Hub https://hub.docker.com/r/clamav/clamav/. Người dùng nên cập nhật bản vá sớm nhất để ngăn chặn bị tấn công.

- Lỗ hổng có PoC: https://github.com/Mattb709/CVE-2025-293Q6-PoC-FoxCMS-RCE.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin góp phần bảo đảm an toàn các cơ quan, đơn vị trên địa bàn tỉnh, Công an tỉnh đề nghị lãnh đạo các đơn vị tiếp tục chỉ đạo rà soát, cập nhật, vá lỗi hệ thống, tăng cường triển khai các biện pháp giám sát liên tục các hệ thống thông tin, phát hiện sớm các dấu hiệu bất thường, tấn công mạng. Trong quá trình thực hiện nếu có khó

khăn, vướng mắc kịp thời liên hệ Công an tỉnh (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, số điện thoại 069.4309.485) để được hỗ trợ.

Đề nghị các đồng chí quan tâm chỉ đạo thực hiện./.

Nơi nhận:
- Như trên;
- Lãnh đạo Công an tỉnh;
- Phòng nghiệp vụ thuộc Công an tỉnh;
- Công an các xã, phường;
- Công an đặc khu Lý Sơn;
- Lưu: VT, ANM(Đ1).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CÔNG AN TỈNH QUẢNG NGÃI

Đại tá Võ Văn Dương