BỘ CÔNG AN
CÔNG AN TỈNH QUẢNG NGÃI

Số: 1074 /CAT-ANM

V/v cảnh báo lỗ hổng bảo mật nghiêm trọng tháng 7/2025

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

Quảng Ngãi, ngày 07 tháng 8 năm 2025

Kính gửi:
- Ủy ban Mặt trận Tổ quốc Việt Nam tỉnh;
- Văn phòng Tỉnh ủy, UBND tỉnh;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Bộ Chỉ huy Quân sự tỉnh; Cục Thi hành án dân sự tỉnh;
- Viện Kiểm sát nhân dân tỉnh; Tòa án nhân dân tỉnh;
- Chi Cục Thống kê tỉnh; Bảo hiểm xã hội tỉnh; Thuế tỉnh;
- Kho bạc Nhà nước tỉnh; Cảng vụ Hàng hải tỉnh;
- Các sở, ban ngành và hội đoàn thể tỉnh;
- UBND các xã, phường, đặc khu;
- Trường Đại học Phạm Văn Đồng, Cao đẳng Cộng đồng Kon Tum, Cao đẳng Việt Nam - Hàn Quốc - Quảng Ngãi;
- Công ty CP Lọc hóa dầu Bình Sơn; Truyền tải điện Quảng Ngãi; Điện lực Quảng Ngãi.

Trong tháng 7/2025, 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 **11** 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; 06 lỗ hổng bảo mật nghiêm trọng; 01 lỗ hổng bảo mật mức trung bình (trong đó 05 lỗ hổng có PoC công khai), cụ thể:

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

*** CVE-2025-6514 -** Lỗ hổng mcp-remote cho phép thực thi mã từ xa trên hệ điều hành Windows

- Mô tả:

+ Điểm CVSS: 9.6/10; Mức độ: Critical;

+ Lỗ hổng này cho phép tin tặc kích hoạt lệnh hệ điều hành tùy ý trên máy chạy mcp-remote khi máy này khởi tạo kết nối với máy chủ MCP không đáng tin cậy, gây ra rủi ro đáng kể cho người dùng và xâm phạm toàn bộ hệ thống.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến các phiên bản mcp-remote từ 0.0.5 đến 0.1.15.

- Khuyến nghị: Quản trị viên cần cập nhật lên phiên bản mcp-remote 0.1.16 để khắc phục lỗ hổng và không kết nối đến máy chủ MCP không đáng tin cậy hoặc không an toàn bằng phiên bản bị ảnh hưởng đều có nguy cơ bị tấn công.

- Lỗ hổng chưa có PoC công khai.

*** CVE-2025-48822** - Lỗ hổng đọc ngoài giới hạn trong Windows Hyper-V

- Mô tả:

+ Điểm CVSS: 8.6/10; Mức độ: High;

+ Lỗ hổng trong Windows Hyper-V (một công nghệ ảo hóa của Microsoft, cho phép chạy nhiều hệ điều hành khác nhau trên cùng một máy tính vật lý như một nền tảng ảo hóa) cho phép tin tặc thực thi mã cục bộ bằng cách đọc ngoài giới hạn bộ nhớ.

- Phiên bản ảnh hưởng: Các phiên bản Windows 10 Version 1809, Windows Server 2019 từ 10.0.17763.0 đến 10.0.17763.7558.

- Khuyến nghị: Microsoft đã báo cáo rằng lỗ hổng này đã được giảm thiểu hoàn toàn và người dùng nên cập nhật lên phiên bản hệ điều hành mới nhất. Hướng dẫn cập nhật : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-48822.

- Lỗ hổng chưa có PoC công khai.

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

*** CVE-2025-32463** - Lỗ hổng Sudo cho phép người dùng quyền truy cập Root trên Linux.

- Mô tả:

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

+ Lỗ hổng này cho phép tin tặc sử dụng tài khoản cục bộ leo thang đặc quyền bằng cách lừa Sudo tải một thư viện dùng chung tùy ý bằng thư mục gốc do người dùng chỉ định thông qua tùy chọn -R(— chroot). Tin tặc có thể chạy các lệnh tùy ý với tư cách root trên các hệ thống hỗ trợ /etc/nsswitch.conf.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến các phiên bản Sudo trước 1.9.17p1.

- Khuyến nghị: Nhà phát hành đã khắc phục trong Sudo phiên bản 1.9.17p1. Người dùng được khuyên nên áp dụng các bản sửa lỗi cần thiết và đảm bảo rằng các bản phân phối máy tính để bàn Linux được cập nhật bằng các gói mới nhất.

- Lỗ hổng có PoC: https://github.com/pr0v3rbs/CVE-2025-32463_chwoot.

3. Lỗ hổng bảo mật phần mềm trên tường lửa

*** CVE-2025-52985** - Lỗ hổng Use of Incorrect Operator trong tường lửa Routing Engine.

- Mô tả:

+ Điểm CVSS: 6.9/10; Mức độ: Medium;

+ Lỗ hổng xảy ra khi bộ lọc tường lửa được áp dụng cho giao diện Io0 hoặc re:mgmt tham chiếu đến danh sách tiền tố với 'from prefix-list', và danh sách tiền

tố đó chứa hơn 10 mục, danh sách tiền tố sẽ không khớp và các gói tin đến hoặc đi từ thiết bị cục bộ sẽ không được lọc. Từ đó cho phép tin tặc không xác thực, hoạt động trên mạng, vượt qua các hạn chế bảo mật.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến Junos OS Evolved: Phiên bản 23.2R2-S3-EVO trước 23.2R2-S4-EVO, Phiên bản 23.4R2-S3-EVO trước 23.4R2-S5-EVO, Phiên bản 24.2R2-EVO trước 24.2R2-S1-EVO, Phiên bản 24.4R2-EVO trước 24.4R1-S3-EVO, 24.4R2-EVO.

- Khuyến nghị: Các bản phát hành phần mềm sau đây đã được cập nhật để giải quyết vấn đề cụ thể này: 23.2R2-S4-EVO, 23.4R2-S5-EVO, 24.2R2-S1-EVO, 24.4R1-S3-EVO, 24.4R2-EVO, 25.2R1-EVO và tất cả các bản phát hành tiếp theo. Nếu người dùng chưa thể cập nhật có thể sử dụng giải pháp thay thế: tham chiếu đến danh sách tiền tố với điều kiện khớp 'source-prefix-list' hoặc 'destination-prefix-list' ('from'). Thông tin chi tiết tại: https://supportportal.juniper.net/s/article/2025-07-Security- Bulletin-Junos-OS-Evolved-When-a-control-plane-firewall-filter-refers-to-a- prefix-list-with-more-then-10-entries-it-s-not-matchinq-CVE-2025-52985.

- Lỗ hổng chưa có PoC công khai.

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

* CVE-2025-25257 - Lỗ hổng SQL Injection không xác thực trong FortiWeb.

- Mô tả:

+ Điểm CVSS: 9.8/10; Mức độ: Critical;

+ Lỗ hổng do việc vô hiệu hóa không đúng cách các thành phần đặc biệt được sử dụng lệnh SQL trong FortiWeb cho phép tin tặc chưa được xác thực thực thi mã hoặc lệnh SQL trái phép thông qua các yêu cầu HTTP hoặc HTTPs được tạo thủ công.

- Phiên bản ảnh hưởng: Các phiên bản FortiWeb bị ảnh hưởng từ 7.6.0 đến 7.6.3, từ 7.4.0 đến 7.4.7, từ 7.2.0 đến 7.2.10 và từ 7.0.0 đếb 7.0.10.

- Khuyến nghị: Fortinet khuyến nghị quản trị viên cần cập nhật ngay hệ thống FortiWeb lên phiên bản đã vá theo hướng dẫn: https://fortiquard.fortinet.com/psirt/FG-IR-25-151. Nếu không thể cập nhật ngay lập tức, Fortinet đề xuất tạm thời tắt giao diện quản trị HTTP/HTTPS như một giải pháp thay thế.

- Lỗ hổng có PoC: https://github.com/0xbiqshaq/CVE-2025-25257.

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

* CVE-2025-6993- Lỗ hổng leo thang đặc quyền WordPress WP Mail.

- Mô tả:

+ Điểm CVSS: 7.5/10; Mức độ: High;

+ Lỗ hổng do ủy quyền không đúng cách trong trình xử lý AJAX get_email_log_details(). Trình xử lý này đọc postjd do máy khách cung cấp và truy xuất nội dung bài đăng nhật ký email tương ứng (bao gồm cả liên kết đặt lại mật khẩu), chỉ dựa vào chức năng 'edit_posts' mà không giới hạn quyền quản trị viên hoặc xác thực quyền sở hữu.

- Phiên bản ảnh hưởng: Các phiên bản Plugin Ultimate WP Mail từ 1.0.17 đến 1.3.6.

- Khuyến nghị: Nhà phát hành đã khắc phục lỗ hổng trong phiên bản Plugin Ultimate WP Mail 1.3.7. 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://wordpress.Org/plugins/ultimate-wp-nnail/#developers.

- Lỗ hổng chưa có PoC công khai.

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

*** CVE-2025-49826** - Lổ hổng bộ nhớ đệm trong Next.js

- Mô tả:

+ Điểm CVSS: 7.5/10; Mức độ:High;

+ Lỗ hổng do lỗi logic xác thực lại bộ nhớ đệm cho cơ chế Tái tạo Tĩnh Gia tăng (ISR). Cho phép lưu trữ phản hồi HTTP 204 cho các trang tĩnh, dẫn đến phản hồi 204 được cung cấp cho tất cả người dùng đang cố gắng truy cập trang, dẫn đến việc ngừng cung cấp dịch vụ cho nội dung quan trọng dành cho người dùng.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến các phiên bản Next.js từ 15.0.4 đến 15.1.8.

- Khuyến nghị: Next.js đã vá lỗi trong phiên bản 15.2.0 và cũng đưa bản sửa lỗi trở lại phiên bản 15.0.4. Người dùng đang chạy phiên bản Next.js tự lưu trữ hoặc tại chỗ từ 15.1.0 đến 15.1.7, cần nâng cấp ngay lên 15.2.0 trở lên. Ngoài ra những người dùng đang sử dụng phiên bản chính cũ hơn, hãy đảm bảo đang sử dụng phiên bản 15.0.4 trở xuống.

- Lỗ hổng chưa có PoC công khai.

7. Lỗ hổng bảo mật phần mềm trên trình duyệt

*** CVE-2025-6558** - Lỗ hổng xác thực không chính xác dữ liệu đầu vào của trình duyệt.

- Mô tả:

+ Điểm CVSS: 8.8/10; Mức độ: High.

+ Lỗ hổng do việc xác thực không đầy đủ dữ liệu đầu vào không đáng tin cậy trong ANGLE và GPU trong Google Chrome trước phiên bản 138.0.7204.15 cho phép tin tặc có khả năng thực hiện thoát khỏi sandbox thông qua một trang HTML được tạo sẵn.

- Phiên bản ảnh hưởng: Lỗ hổng bảo mật này ảnh hưởng đến các phiên bản Google Chrome trước 138.0.7204.157.

- Khuyến nghị: Nhà phát hành khuyến nghị người dùng nên cập nhật trình duyệt Chrome lên phiên bản 138.0.7204.157/.158 cho Windows và Apple macOS, và 138.0.7204.157 cho Linux. Để đảm bảo các bản cập nhật mới nhất đã được cài đặt, người dùng có thể truy cập mục Thêm > Trợ giúp > Giới thiệu về Google Chrome và chọn Khởi chạy lại. Thông tin chi tiết tại: https://chromereleases.qooqlebloq.com/2025/07/stable- channel-update-for-desktop_15.html.

- Lỗ hổng chưa có PoC công khai.

*** CVE-2025-6554** - Lỗ hổng Zero-Day nhầm lẫn kiểu dữ liệu đọc/ghi trên Chrome.

- Mô tả:

+ Điểm CVSS: 8.1/10; Mức độ: High.

+ Lỗ hổng do nhầm lẫn kiểu trong công cụ JavaScript V8 cho phép tin tặc thực hiện các thao tác đọc và ghi tùy ý thông qua một trang HTML được thiết kế đặc biệt. Điều này cho phép tin tặc có khả năng thao túng nội dung bộ nhớ, dẫn đến việc thực thi mã tùy ý.

- Phiên bản ảnh hưởng: Lỗ hổng bảo mật này ảnh hưởng đến các phiên bản Google Chrome trước 138.0.7204.157.

- Khuyến nghị: Nhà phát hành khuyến nghị người dùng nên cập nhật trình duyệt Chrome lên phiên bản 138.0.7204.96/.97 cho Windows, 138.0.7204.92/.93 cho macOS và 138.0.7204.96 cho Linux. Thông tin chi tiết tại: https://chromereleases.googleblog.com/2025/Q6/stable-channel-update-for-desktop_30.html.

- Lỗ hổng có PoC: https://gist.github.com/mistymntncop/37c652c2bf7373b4aa33bb50f52ee0f2.

8. Lỗ hổng bảo mật chuỗi cung ứng khác

*** CVE-2025-6965** – Lỗ hổng lỗi bộ nhớ trong hệ quản trị cơ sở dữ liệu SQLite.

- Mô tả:

+ Điểm CVSS: 7.2/10; Mức độ: High;

+ Lỗ hổng trong SQLite khiến số lượng thuật ngữ tổng hợp có thể vượt quá số cột khả dụng dẫn đến lỗi bộ nhớ. Tin tặc có thể chèn các câu lệnh SQL tùy ý vào ứng dụng có thể gây ra lỗi tràn số nguyên dẫn đến việc đọc phần cuối của một mảng.

- Phiên bản ảnh hưởng: Các phiên bản SQLite trước 3.50.2.

- Khuyến nghị: Nhà phát hành SQLite khuyến nghị người dùng nâng cấp lên phiên bản 3.50.2 trở lên để khắc phục lỗ hổng, mọi thông tin về lỗ hổng:

https://www.sqlite.org/src/info/5508b56fd24016c13981ec280ecdd8330Q7c9d8d d595edb295b984c2b487b5c8.

- Lỗ hổng có PoC: https://github.com/advisories/ghsa-ir5f-v2iv-69x6.

*** CVE-2025-53770** - Lỗ hổng thực thi mã từ xa của Microsoft SharePoint Server.

- Mô tả:

+ Điểm CVSS: 9.8/10; Mức độ: Critical;

+ Lỗ hổng này khai thác lỗi bỏ qua xác thực được kích hoạt bằng cách đặt tiêu đề "Referer" thành "/Jayouts/SignOut.aspx". Sau đó được khai thác đế kích hoạt thực thi mã từ xa thông qua 7_layouts/15/ToolPane.aspx".

- Phiên bản ảnh hưởng: Các phiên bản Microsoft SharePoint Server 2019 và Microsoft SharePoint Enterprise Server 2016.

- Khuyến nghị: Microsoft đã phát hành các bản cập nhật bảo mật bảo vệ toàn diện khách hàng sử dụng SharePoint Subscription Edition và SharePoint 2019. Khách hàng nên cập nhật ngay lập tức để đảm bảo an toàn. Microsoft đang tích cực phát triển các bản cập nhật cho SharePoint 2016. Hướng dẫn đầy đủ và chi tiết phát hiện có sẵn trên blog: https://msrc.microsoft.com/bloq/2025/07/customer-quidance-for-sharepoint- vulnerability-cve-2025-53770/.

- Lỗ hổng có PoC: https://github.com/hazcod/CVE-20025-53770.

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 088.830.9485) để được hỗ trợ.

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

Nơi nhận:
- Như trên;
- UBND tỉnh (báo cáo);
- Giám đốc CA tỉnh;
- Phòng Tham mưu;
- Lưu: VT, ANM.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
CÔNG AN TỈNH QUẢNG NGÃI

Đại tá Võ Văn Dương