BỘ CÔNG AN
CÔNG AN TỈNH QUẢNG NGÃI

Số: 4836/CAT-ANM

V/v cảnh báo lỗ hổng bảo mật nghiêm trọng tháng 11/2025

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

Quảng Ngãi, ngày 25 tháng 12 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;
- Các sở, ban ngành và hội đoàn thể tỉnh;
- Bộ Chỉ huy Quân sự tỉnh; Tòa án nhân dân tỉnh;
- Viện Kiểm sát nhân dân tỉnh; Thi hành án dân sự tỉnh;
- Bảo hiểm xã hội tỉnh; Cảng vụ Hàng hải Quảng Ngãi;
- Thống kê tỉnh; Thuế tỉnh Quảng Ngãi;
- Kho bạc Nhà nước khu vực XV;
- Báo và Phát thanh, Truyền hình Quảng Ngãi;
- UBND các xã, phường, Đặc khu Lý Sơn.
- Các Trường: Đại học Phạm Văn Đồng, Cao đẳng 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 11/2025, 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 03 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; 04 lỗ hổng đã công khai PoC, cụ thể:

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

1.1. CVE-2025-60710 - Lỗ hổng leo thang đặc quyền trong Windows Tasks

- Mô tả:

+ Điểm CVSS: 7.8/10;

+ Mức độ: High;

+ Lỗ hổng xảy ra trong \Microsoft\Windows\WindowsAI\Recall \PolicyConfiguration của Windows Tasks, cho phép tin tặc khai thác lỗi phân giải liên kết không đúng trước khi truy cập tệp trong tác vụ theo lập lịch của Windows AI Recall, cho phép xóa thư mục tùy ý với quyền Admin thông qua thao tác trên các liên kết thư mục và liên kết, có thể được sử dụng để leo thang đặc quyền.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến các phiên bản của Windows 11 Phiên bản 25H2 từ 10.0.26200.0 đến trước 10 0.26200.717.

- Khuyến nghị: Microsoft đã phát hành bản cập nhật bảo mật để giải quyết lỗ hổng này như một phần của bản cập nhật Patch Tuesday tháng 11 năm 2025. Người dùng được khuyến cáo áp dụng bản cập nhật bảo mật KB5068861 cho các hệ thống Windows bị ảnh hưởng để giảm thiểu lỗ hổng này. Thông tin chi tiết về lỗ hổng: https://msrc.microsoft.com/update-guide/vulnerabilitv/CVE-2025-60710.

- Lỗ hổng có PoC: https://github.com/redpack-kr/CVE-2025-60710.

1.2. CVE-2025-59287 – Lỗ hổng thực thi mã từ xa của Windows Server Update Service (WSUS).

- Mô tả:

+ Điểm CVSS: 9.8/10;

+ Mức độ: Critial;

+ Lỗ hổng được phát hiện trong Dịch vụ Cập nhật Máy chủ Windows (WSUS) của Microsoft, một thành phần cốt lõi của doanh nghiệp dùng để quản lý bản vá. Lỗ hổng cho phép tin tặc chưa được xác thực gửi các yêu cầu được tạo sẵn đến các điểm cuối WSUS trên cổng 8530 và 8531 và thực thi mã. Các máy chủ bị khai thác chạy các payload PowerShell để liệt kê thông tin hệ thống và trích xuất dữ liệu ra các webhook bên ngoài.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến các phiên bản Microsoft Windows Server 2012, 2012 R2, 2016, 2019, 2022 (bao gồm cả Phiên bản 23H2) và 2025.

- Khuyến nghị: Microsoft đã phát hành bản cập nhật bảo mật cho các phiên bản Windows Server được hỗ trợ sau: Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows Server 2022, Phiên bản 23H2 (cài đặt Server Core) và Windows Server 2025. Sau khi bản vá được cài đặt, người dùng nên khởi động lại hệ thống để bản cập nhật có hiệu lực. Nếu không thể áp dụng chế độ "out-of-band", người dùng có thể thực hiện các hành động sau đây để bảo vệ khỏi lỗ hổng:

+ Vô hiệu hóa WSUS Server Role trong máy chủ (nếu được bật).

+ Chặn lưu lượng truy cập đến Cổng 8530 và 8531 trên tường lửa máy chủ.

Thông tin chi tiết bản cập nhật: https://support.microsoft.com/en-us/topic/october-23-2025-kb5070882-os-build-14393-8524-out-of-band-3400c459-db78-48bc-ae69-f61bff15ea7c.

- Lỗ hổng có PoC: https://github.com/keeganparr1/CVE-2025-59287-hawktrace.

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

CVE-2025-61667 – Lỗ hổng leo thang đặc quyền trên Datadog Linux Host Agent.

- Mô tả:

+ Điểm CVSS: 7.8/10;

+ Mức độ: High;

+ Lỗ hổng bảo mật bắt nguồn do không đủ quyền được thiết lập trên thư mục 'opt/datadog-agent/python-scripts/_pycache_' trong quá trình cài đặt. Mã trong thư mục này chỉ được Agent chạy trong quá trình cài đặt/nâng cấp Agent. Điều này có thể cho phép tin tặc có quyền truy cập cục bộ sửa đổi các tệp trong thư mục này, sau đó sẽ được chạy khi Agent được nâng cấp, dẫn đến leo thang đặc quyền cục bộ.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến các phiên bản Datadog Linux Host Agent phiên bản 7.65.0 đến 7.70.2.

- Khuyến nghị: Datadog đã giải quyết vấn đề này trong phiên bản 7.71.0 bằng cách sửa quyền thư mục để ngăn chặn các sửa đổi trái phép. Người dùng nên cập nhật ngay lập tức, trường hợp chưa thể cập nhật hãy hạn chế quyền truy cập cục bộ vào các máy chủ đang chạy dễ bị tấn công bằng cách thực thi các biện pháp kiểm soát truy cập nghiêm ngặt và giám sát các hoạt động đáng ngờ.

- Lỗ hổng chưa có PoC công khai.

3. Lỗ hổng bảo mật phần mềm trên tường lửa

CVE-2025-4619 – Lỗ hổng PAN-OS cho phép khởi động lại tường lửa không cần xác thực qua một gói tin

- Mô tả:

+ Điểm CVSS: 6.6/10;

+ Mức độ: Medium;

+ Lỗ hổng này xuất phát từ việc tin tặc có thể khởi động lại tường lửa bằng cách gửi một gói tin được thiết kế đặt biệt. Việc khởi động lại nhiều lần sẽ khiến tường lửa chuyển sang chế độ bảo trì, từ chối dịch vụ (DoS).

- Phiên bản ảnh hưởng: Lỗ hổng này ảnh hưởng các phiên bản PAN-OS 11.2 từ 11.2.0 đến 11.2.4, PAN-OS 11.1 từ 11.1 0 đến 11.1.6, PAN-OS 10.2 từ 10.2.0 đến 10.2.13.

- Khuyến nghị: Palo Alto Networks khuyến nghị người dùng nâng cấp lên một trong các bản vá lỗi nóng hoặc bản bảo trì được liệt kê: PAN-OS 11.2 phiên bản 11.2.5 hoặc phiên bản mới hơn, PAN-OS 11.1 phiên bản 11.1.7 hoặc phiên bản cao hơn, PAN-OS 10.2 phiên bản 10.2.14 hoặc phiên bản mới hơn. Chi tiết bản cập nhật: https://securitv.paloaltonetworks.com/CVE-2025-4619.

- Lỗ hổng chưa có PoC công khai.

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

CVE-2025-9501 – Lỗ hổng của W3 Total Cache gây RCE không xác thực trên WordPress

- Mô tả:

+ Điểm CVSS: 9/10;

+ Mức độ: Critial;

+ Lỗ hổng này cho phép tin tặc tấn công từ xa bằng cách để lại bình luận trên bất kỳ bài đăng công khai nào và nếu dữ liệu được phân tích, trang web sẽ thực thi các lệnh PHP do kẻ tấn công cung cấp - có khả năng cấp quyền kiểm soát toàn bộ trang web, đánh cắp dữ liệu hoặc cài đặt backdoor và mã độc. Cuộc tấn công này không yêu cầu đăng nhập, không cần đặc quyền và không cần vượt qua CAPTCHA, khiến nó có thể dễ dàng bị khai thác trên các trang web không được bảo vệ.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến các phiên bản W3 Total Cache từ 2.8.13 trở xuống.

- Khuyến nghị: Nhà phát hành thông báo lỗ hổng bảo mật này đã được vá hoàn toàn trong W3 Total Cache phiên bản 2.8.13 và tất cả chủ sở hữu trang web được khuyến cáo cập nhật ngay lập tức. Thông tin bản cập nhật có trong: https://wordpress.org/plugins/w3- total-cache/.

- Lỗ hổng chưa có PoC công khai.

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

CVE-2025-61084 - Lỗ hổng giả mạo email của MDaemon Mail Server

- Mô tả:

+ Điểm CVSS: 7.1/10;

+ Mức độ: High;

+ Lỗ hổng xảy ra do MDaemon chỉ xác thực địa chỉ bên trong dấu ngoặc nhọn, tin tặc có thể tạo một From: tiêu đề với nhiều khoảng trắng Unicode vô hình để hiển thị người gửi giả mạo trong khi vượt qua xác thực, các biện pháp bảo vệ SPF/DKIM/DMARC, cho phép giả mạo email ngay cả khi đã áp dụng các biện pháp bảo vệ chống giả mạo.

- Phiên bản ảnh hưởng: Lỗ hổng bào mật này ảnh hưởng đến các phiên bản MDaemon Mail Server trước 23.5.2.

- Khuyến nghị: Nhà phát hành hiện nay chưa có bản vá nào khắc phục lỗ hổng bởi lý do việc giả mạo giao diện người dùng (UI) xảy ra trên máy khách, chứ không phải trên máy chủ như sản phẩm của MDaemon hoặc bất kỳ triển khai máy chủ nào khác. Người dùng khuyến nghị tạm thời sử dụng tính năng Header Screening trong sản phẩm của MDaemon có thể được sử dụng để giảm thiểu lỗ hổng phía máy khách.

- Lỗ hổng có PoC: https://github.com/x00nullbit/CVE-References/tree/main/CVE- 2025-61084.

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

CVE-2025-62518 – Lỗ hổng thực thi mã từ xa trong thư viện Rust Async-Tar

- Mô tả:

+ Điểm CVSS: 8.1/10;

+ Mức độ: High;

+ Lỗ hổng bảo mật này là lỗi không đồng bộ trong async-tar/tokio-tar cho phép tin tặc "lén" lồng các tệp từ TAR vào phần trích xuất bên ngoài bằng cách khai thác sự không khớp giữa tiêu đề PAX và ustar (PAX hiển thị kích thước thực, ustar hiển thị 0). Việc khai thác cũng có thể cho phép ghi đè tệp trong quá trình trích xuất và vượt qua trình quét bảo mật.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến tất cả các phiên bản astral-tokio-tar trước 0.5.6.

- Khuyến nghị: Nhà phát hành khuyến cáo các tổ chức sử dụng thư viện Rust bị ảnh hưởng nên nâng cấp lên astral-tokio-tar phiên bản 0.5.6 trở lên hoặc không sử dụng các nhánh thư viện như tokio-tar. Nếu không thể vá lỗi ngay lập tức, hãy áp dụng các biện pháp giảm thiểu như sử dụng sandbox, giới hạn kích thước tệp và quét sau khi trích xuất, đồng thời xem xét các mối quan hệ phụ thuộc để phát hiện các mối đe dọa gián tiếp.

- Lỗ hổng có PoC: https://github.com/edera-dev/cve-tarmageddon.

7. Lỗ hổng bảo mật phần mềm trên trình duyệt

CVE-2025-13223 – Lỗ hổng Zero-Day trong JavaScript V8 của Chrome

- Mô tả:

+ Điểm CVSS: 8.8/10;

+ Mức độ: High;

+ Lỗ hổng xảy ra khi một chương trình sai kiểu dữ liệu của một đối tượng, dẫn đến lỗi logic và diễn giải sai bộ nhớ trong trung tâm xử lý web của Chrome. Điều này có nghĩa là tin tặc có thể khai thác lỗ hổng bảng cách tạo một trang HTML đặc biệt và lừa người dùng truy cập vào, từ đó tin tặc có thể thực hiện lỗi heap và thực thi mã tuỳ ý từ xa.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến các phiên bản Chrome 142.0.7444.175/.176 trở xuống.

- Khuyến nghị: Nhà phát hành khuyến cáo tất cả người dùng Chrome trên Windows, Mac và Linux nên cập nhật ngay lên phiên bản ổn định mới: 142.0.7444.175/.176 (Windows), 142.0.7444.176 (Mac) và 142.0.7444.175 (Linux). Hướng dẫn chi tiết: mở Chrome, chọn menu ba chấm (...) > Trợ giúp > Giới thiệu về Google Chrome. Trình duyệt sẽ tự quét, tải và yêu cầu khởi động lại để áp dụng bản vá. Chi tiết bản cập nhật: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-13223.

- Lỗ hổng chưa có PoC công khai.

8. Lỗ hổng bảo mật khác

8.1. CVE-2025-43431 – Lỗ hổng gây lỗi bộ nhớ trong WebKit của Apple

- Mô tả:

+ Điểm CVSS: 8.8/10;

+ Mức độ: High;

+ Lỗ hổng này được xác định là lỗi hỏng bộ nhớ trong WebKit, công cụ trình duyệt của Apple, ảnh hưởng đến nhiều hệ điều hành Apple, bao gồm macOS, iOS và iPadOS. Tin tặc có thể khai thác lỗ hổng bằng cách truy cập vào các trang web có nội dung độc hại mà trình duyệt không thể xử lý dẫn tới hỏng bộ nhớ trong của hệ thống.

- Phiên bản ảnh hưởng: Lỗ hổng bảo mật này ảnh hưởng đến các phiên bản IOS và IpadOS trước phiên bản 18.7.

- Khuyến nghị: Apple đã khắc phục lỗ hổng này bằng cách triển khai các cơ chế xử lý bộ nhớ được cải thiện trong các hệ thống bị ảnh hưởng. Người dùng được khuyến cáo cập nhật lên Safari 26.1, iOS 18.7.2, iPadOS 18.7.2 hoặc macOS Tahoe 26.1. Chi tiết về bản cập nhật: https://support.apple.com/en-us/125633.

- Lỗ hổng chưa có PoC công khai.

8.2. CVE-2025-6542 – Lỗ hổng Command Injection trên cổng Omada trên thiết bị TP-link

- Mô tả:

+ Điểm CVSS: 9.3/10;

+ Mức độ: Critial;

+ Lỗ hổng ảnh hưởng đến các thiết bị TP-Link Omada Gateway, được triển khai rộng rãi trong các mạng doanh nghiệp và doanh nghiệp vừa và nhỏ (SMB) cho mục đích định tuyến, VPN và quản lý mạng. Lỗ hổng này, được phân loại là lỗ hổng Tiêm lệnh Từ xa (Remote Command Injection), cho phép tin tặc thực thi các lệnh hệ điều hành tùy ý bằng cách khai thác lỗi xác thực đầu vào không hợp lệ trong giao diện quản lý web của thiết bị gây ra rủi ro nghiêm trọng cho cơ sở hạ tầng và bảo mật dữ liệu của tổ chức.

- Phiên bản ảnh hưởng:

+ Lỗ hổng bảo mật này ảnh hưởng đến nhiều mẫu TP-Link Omada Gateway.

+ ER707-M2: phiên bản cũ hơn 1.3.1 Bản dựng 20251009 Rel.67687.

+ ER8411: phiên bản cũ hơn 1.3.3 Bản dựng 20251013 Rel.44647.

+ ER605 V2: phiên bản cũ hơn 2 2.3 Bản dựng 20251008 Rel.12231.

+ ER7206: phiên bản cũ hơn 1.4.3 Bản dựng 20251009 Rel.53521.

- Khuyến nghị: Nhà phát hành khuyến cáo các tổ chức phải nâng cấp các thiết bị bị ảnh hưởng lên phiên bản mới nhất, hạn chế quyền truy cập quản lý web vào các mạng đáng tin cậy, thực thi thông tin xác thực quản trị mạnh, vô hiệu hóa các dịch vụ không cần thiết và liên tục theo dõi các nỗ lực khai thác. Thông tin chi tiết về lỗ hổng: https://support.omadanetworks.com/en/document/108455/.

- Lỗ hổng chưa có PoC công khai.

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;
- Giám đốc Công an tỉnh (báo cáo);
- Phòng Tham mưu;
- Lưu: VT, ANM.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Đại tá Võ Văn Dương