BỘ CÔNG AN **CÔNG AN TP HẢI PHÒNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 14102 /CAHP-ANM V/v thông báo tình hình an ninh mạng tháng 10/2026	*Hải Phòng, ngày28 tháng 10 năm 2026*

Kính gửi:
- Các cơ quan Đảng thành phố;
- Các cơ quan Trung ương đóng tại địa phương;
- Các sở, ban, ngành thành phố;
- UBND các xã, phường, đặc khu;
- Các đơn vị sự nghiệp thành phố;
- Các tổ chức chính trị, xã hội, doanh nghiệp.

Thực hiện chức năng quản lý nhà nước về an ninh mạng trên địa bàn thành phố, qua công tác nắm tình hình, Công an thành phố Hải Phòng thông báo một số nội dung như sau:

I. TÌNH HÌNH AN NINH MẠNG TRÊN ĐỊA BÀN THÀNH PHỐ

1. Công tác bảo đảm an ninh mạng

- Từ ngày 06/10 đến ngày 09/10/2026, Công an thành phố đã tổ chức Hội nghị tập huấn và diễn tập an ninh mạng trên địa bàn thành phố Hải Phòng năm 2026, với sự tham gia của các chuyên gia, giảng viên, báo cáo viên và gần 200 cán bộ phụ trách công nghệ thông tin, an ninh mạng của các sở, ban, ngành, địa phương và doanh nghiệp trên địa bàn thành phố. Hội nghị nhằm cập nhật kiến thức, nâng cao kỹ năng phát hiện, phối hợp xử lý, ứng cứu sự cố an ninh mạng cho đội ngũ cán bộ làm công tác bảo đảm an ninh mạng tại các cơ quan, đơn vị.

- Công an thành phố đã phát hiện tình trạng mất an ninh mạng liên quan đến hệ thống thông tin của Công ty Cổ phần Vận tải biển Việt Nam (Vosco) và Sở Văn hóa, Thể thao và Du lịch thành phố.

- Công an thành phố đã phối hợp với các đơn vị xử lý, khắc phục sự cố tấn công mã hóa dữ liệu (ransomware) xảy ra tại Bệnh viện Phổi Hải Phòng.

2. Kết quả giám sát an ninh mạng tại Trung tâm dữ liệu thành phố

Trong tháng, hệ thống thông tin đặt tại Trung tâm dữ liệu thành phố không ghi nhận sự cố an ninh mạng nghiêm trọng; các cảnh báo phát sinh đã được tiếp nhận, phân tích và xử lý theo quy trình.

3. Kết quả Hệ thống quản lý mã độc tập trung thành phố

Trong tháng 10/2026, Hệ thống quản lý mã độc tập trung thành phố đã phát hiện, ngăn chặn 180 mối đe dọa (mã độc, liên kết giả mạo) và 8.001 tệp tin độc hại trên 308 thiết bị thuộc 92 cơ quan, tổ chức trên địa bàn thành phố.

4. Một số phương thức, thủ đoạn tấn công và tin tức an ninh mạng đáng chú ý

- Bảo hiểm xã hội Việt Nam cảnh báo thủ đoạn mạo danh cán bộ bảo hiểm xã hội, công an, chính quyền địa phương, lợi dụng nhu cầu tra cứu thông tin, giải quyết chế độ bảo hiểm xã hội, bảo hiểm y tế của người dân để lừa đảo. Các đối tượng thường hối thúc người dân cài đặt ứng dụng VssID giả mạo (tệp .apk) nhằm chiếm quyền điều khiển điện thoại, đánh cắp mã OTP, thông tin tài khoản ngân hàng để chiếm đoạt tài sản.

- Microsoft đã triệt phá dịch vụ lừa đảo qua thư điện tử Evil Tokens - nền tảng sử dụng trí tuệ nhân tạo (AI) đã xâm nhập hơn 12.000 hộp thư của trên 10.000 tổ chức trên thế giới; thu giữ 50 trang web, vô hiệu hóa hơn 150 tên miền, bắt giữ 02 đối tượng tại Anh. Chatbot AI của Evil Tokens có khả năng phân tích nội dung hộp thư, xác định các giao dịch thanh toán để lập kịch bản gian lận tài chính; đồng thời lợi dụng cơ chế xác thực bằng mã thiết bị (device code) của Microsoft để chiếm quyền truy cập tài khoản mà không cần mật khẩu.

- Apple đã phát hành bản cập nhật iOS, macOS để vá lỗ hổng zero-day CVE-2026-86950 trong thành phần CoreGraphics. Lỗ hổng cho phép thực thi mã tùy ý, đang bị khai thác trong các cuộc tấn công có chủ đích, rất tinh vi nhằm vào một số cá nhân cụ thể; ảnh hưởng nhiều thiết bị từ iPhone 11 trở lên và iPad.

II. CẢNH BÁO CÁC LỖ HỔNG BẢO MẬT

Trong tháng 10/2026, các hãng công nghệ, tổ chức an ninh mạng đã công bố một số lỗ hổng bảo mật đáng chú ý sau:

STT	Lỗ hổng, sản phẩm ảnh hưởng	Mô tả, nguy cơ	Mức độ
1	02 lỗ hổng PHP2Shell (CVE-2026-109618, CVE-2026-109619) trong PHP	Lỗ hổng trong lõi PHP (cơ chế xử lý lỗi hết bộ nhớ và lỗi nghiêm trọng khi tiếp nhận yêu cầu), cho phép đối tượng thực thi mã từ xa trên máy chủ mà không cần xác thực; điểm CVSS v4.0: 9.2/10. Ảnh hưởng các phiên bản PHP trước 8.2.35, 8.3.36, 8.4.27, 8.5.12 và các phiên bản cũ hơn (7.4, 8.0, 8.1). Mã khai thác đã được công bố; hoạt động dò quét, khai thác diện rộng được ghi nhận ngay sau	**Đặc biệt nghiêm trọng**

STT	Lỗ hổng, sản phẩm ảnh hưởng	Mô tả, nguy cơ	Mức độ
		khi lỗ hổng công bố ngày 21/10/2026, trong đó có hành vi cài mã độc botnet Mirai.	
2	Lỗ hổng zero-day CVE-2026-86950 trên iOS, macOS	Lỗ hổng trong thành phần CoreGraphics, cho phép thực thi mã tùy ý; đang bị khai thác trong các cuộc tấn công có chủ đích, tinh vi nhằm vào một số cá nhân cụ thể. Ảnh hưởng iPhone 11 trở lên và iPad. Apple đã phát hành bản vá.	Nghiêm trọng
3	10 lỗ hổng bảo mật trong Node.js	Được vá trong đợt cập nhật bảo mật cho 03 nhánh phát hành 26.x, 24.x và 22.x; trong đó có 04 lỗ hổng mức cao, ảnh hưởng các thành phần cốt lõi như tra cứu DNS, kiểm tra chứng chỉ TLS và giải nén dữ liệu Brotli.	Trung bình đến Cao
4	Lỗ hổng CVE-2026-96940 trong Microsoft Exchange Server	Nếu khai thác thành công, đối tượng có thể truy cập trái phép hộp thư của người dùng khác trong cùng tổ chức, đọc thư và tệp đính kèm. Microsoft đã phát hành bản vá.	Nghiêm trọng
5	Lỗ hổng CVE-2026-99999 (PwnEscape) trong nhân Linux	Cho phép mã chạy trong máy ảo khách đọc bộ nhớ của máy chủ ảo hóa, làm sập máy chủ, thậm chí thực thi mã trên máy chủ. Điều kiện khai thác: đối tượng đã có quyền chạy mã trong máy ảo khách; hiện chưa ghi nhận khai thác trong thực tế.	Nghiêm trọng
6	03 lỗ hổng trên camera TP-Link Tapo C200	Gồm: lỗ hổng vượt qua xác thực (CVE-2026-15315) cho phép đối tượng trong cùng mạng chiếm quyền quản trị mà không cần mật khẩu; lỗ hổng từ chối dịch vụ (CVE-2026-15316) làm ngừng dịch vụ quản lý camera; 01 lỗ hổng chưa công bố chi tiết cho phép chiếm quyền điều khiển hoàn toàn camera, lợi dụng để tấn công các thiết bị khác trong mạng.	Nghiêm trọng

Đặc biệt lưu ý đối với 02 lỗ hổng PHP2Shell (CVE-2026-109618, CVE-2026-109619): PHP được sử dụng rất phổ biến trong các cổng/trang thông tin điện tử, hệ thống quản lý văn bản, dịch vụ công trực tuyến và các nền tảng mã nguồn mở như WordPress, Joomla, Drupal, Laravel...; lỗ hổng có thể bị khai thác trực

tiếp từ Internet mà không cần xác thực, mã khai thác đã công khai và đang bị dò quét diện rộng. Đề nghị các cơ quan, đơn vị, địa phương khẩn trương thực hiện:

- Rà soát toàn bộ máy chủ, ứng dụng web có sử dụng PHP thuộc phạm vi quản lý (kể cả hệ thống do doanh nghiệp cung cấp dịch vụ, thuê ngoài vận hành); xác định phiên bản PHP đang sử dụng.

- Nâng cấp ngay lên phiên bản đã được vá: PHP 8.2.35, 8.3.36, 8.4.27, 8.5.12 hoặc mới hơn; đối với các phiên bản 7.4, 8.0, 8.1 đã hết hỗ trợ, cập nhật bản vá của nhà cung cấp hệ điều hành và xây dựng lộ trình nâng cấp lên phiên bản còn được hỗ trợ; khởi động lại toàn bộ tiến trình PHP (PHP-FPM, máy chủ web) sau khi cập nhật.

- Trường hợp chưa thể nâng cấp ngay, áp dụng biện pháp giảm thiểu tạm thời: tắt tính năng theo dõi tiến trình tải tệp (session.upload_progress.enabled = 0); giới hạn kích thước yêu cầu tại máy chủ web, proxy; bật tường lửa ứng dụng web (WAF); hạn chế công khai ra Internet các ứng dụng không cần thiết; tăng cường giám sát nhật ký hệ thống. Các biện pháp này chỉ mang tính tạm thời, không thay thế việc cập nhật bản vá.

- Kiểm tra dấu hiệu bị xâm nhập (tệp lạ, webshell trong thư mục ứng dụng, tiến trình, kết nối bất thường, tài khoản quản trị mới khởi tạo...); trường hợp phát hiện dấu hiệu bị khai thác, khẩn trương cô lập hệ thống và thông báo ngay cho Công an thành phố (qua Phòng An ninh mạng) để phối hợp xử lý.

Đối với các lỗ hổng còn lại, đề nghị các cơ quan, đơn vị, địa phương rà soát sản phẩm, dịch vụ trong phạm vi quản lý; cập nhật kịp thời bản vá của nhà sản xuất (hệ điều hành iOS, macOS; Node.js; Microsoft Exchange Server; nhân Linux trên máy chủ ảo hóa; firmware camera giám sát). Trường hợp chưa thể cập nhật ngay, phải áp dụng biện pháp giảm thiểu rủi ro như giới hạn truy cập, tăng cường giám sát, sao lưu dữ liệu.

III. CÔNG TÁC BẢO ĐẢM AN NINH MẠNG TRONG THỜI GIAN TỚI

Trong thời gian tới, Công an thành phố đề nghị các cơ quan, đơn vị, địa phương quan tâm triển khai một số nội dung sau:

- Khẩn trương rà soát, khắc phục 02 lỗ hổng PHP2Shell nêu tại Mục II; phối hợp với Công an thành phố triển khai dịch vụ giám sát an ninh mạng (SOC) đối với hệ thống thông tin của cơ quan, đơn vị.

- Rà soát tổng thể hệ thống thông tin thuộc phạm vi quản lý; tập trung nguồn lực khắc phục lỗ hổng bảo mật, ưu tiên xử lý trước các lỗ hổng mức nghiêm trọng, mức cao và lỗ hổng đang bị hoặc có nguy cơ cao bị khai thác; cập nhật đầy đủ, kịp thời bản vá bảo mật cho hệ điều hành, phần mềm máy chủ, ứng dụng web, cơ sở dữ

liệu, thiết bị mạng và thiết bị bảo mật; thay đổi mật khẩu mặc định, mật khẩu yếu; gỡ bỏ dịch vụ, tài khoản không cần thiết; định kỳ sao lưu dữ liệu quan trọng theo quy định.

Công an thành phố Hải Phòng đề nghị các cơ quan, đơn vị, địa phương quan tâm, phối hợp triển khai thực hiện. Quá trình thực hiện nếu có khó khăn, vướng mắc, đề nghị liên hệ Công an thành phố (*qua Phòng An ninh mạng; địa chỉ: số 55 Bến Bính, phường Hồng Bàng, thành phố Hải Phòng; số điện thoại: 069.278.5415*) để được hướng dẫn, hỗ trợ./.

Nơi nhận:
- Như trên;
- Cục A05-BCA
- Đ/c Giám đốc CATP (để báo cáo);
- Lưu VT; ANM(Đ4).

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CÔNG HOÀ X.H.C.N VIỆT NAM
CÔNG AN THÀNH PHỐ HẢI PHÒNG

Đại tá Lê Đức Thành