BỘ CÔNG AN
CÔNG AN TỈNH THÁI NGUYÊN

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

Số: 407/CAT-PA05

Thái Nguyên, ngày 26 tháng 01 năm 2026

V/v cảnh báo lỗ hổng bảo mật nghiêm trọng trên các sản phẩm Fortinet

Kính gửi:
- Các sở, ban, ngành thuộc tỉnh;
- UBND các xã, phường.

Qua công tác bảo đảm an toàn, an ninh mạng; rà soát, nắm tình hình trên không gian mạng, Công an tỉnh Thái Nguyên phát hiện thông tin về các lỗ hổng bảo mật nghiêm trọng ảnh hưởng tới một số sản phẩm của hãng Fortinet[1] (FortiSIEM, FortiFone, FortiOS, FortiSwitchManager) đã được công khai trên không gian mạng, tiềm ẩn nguy cơ bị các đối tượng lợi dụng để thực hiện hành vi xâm nhập, tấn công mạng vào hệ thống thông tin của cơ quan, tổ chức.

Do các thiết bị/sản phẩm Fortinet thường được triển khai tại vị trí trọng yếu trong hạ tầng mạng (cửa ngõ kết nối Internet, hệ thống giám sát tập trung, dịch vụ quản trị), khi phát sinh lỗ hổng bảo mật nghiêm trọng có thể bị khai thác từ xa sẽ tiềm ẩn nguy cơ ảnh hưởng lớn đến an toàn, an ninh mạng của cơ quan, đơn vị, địa phương, cụ thể như sau:

- Lỗ hổng CVE-2025-64155 (CVSS 9.4) – Lỗ hổng OS Command Injection trên FortiSIEM, có thể bị khai thác bởi đối tượng tấn công không cần xác thực thông qua các yêu cầu TCP được tạo lập đặc biệt để thực thi lệnh/mã từ xa.

- Lỗ hổng CVE-2025-47855 (CVSS 9.3) – Lỗ hổng trên Web Portal của FortiFone, có thể bị khai thác không cần xác thực thông qua các yêu cầu HTTP/HTTPS được tạo lập đặc biệt nhằm làm lộ cấu hình thiết bị.

- Lỗ hổng CVE-2025-25249 (CVSS 7.4) – lỗi heap-based buffer overflow trong thành phần cw_acd daemon của FortiOS và FortiSwitchManager, có thể dẫn đến thực thi lệnh/mã từ xa không cần xác thực thông qua các yêu cầu được tạo lập đặc biệt.

Các lỗ hổng nêu trên tiềm ẩn nguy cơ bị lợi dụng để xâm nhập, chiếm quyền điều khiển thiết bị, đánh cắp thông tin cấu hình, làm bàn đạp mở rộng tấn công vào hệ thống mạng nội bộ, gây ảnh hưởng nghiêm trọng đến hoạt động

---

[1] Fortinet là hãng cung cấp các giải pháp an toàn thông tin phổ biến hiện nay; trong đó các sản phẩm như FortiGate (tường lửa/Firewall), FortiOS (hệ điều hành vận hành trên thiết bị FortiGate), FortiSIEM (hệ thống giám sát, phân tích, quản lý sự kiện an ninh mạng – SIEM), FortiFone (thiết bị/giải pháp thoại IP) và một số sản phẩm liên quan đang được nhiều cơ quan, đơn vị triển khai để phục vụ công tác quản trị mạng, bảo vệ hệ thống thông tin.

bình thường của các hệ thống thông tin.

Từ tình hình trên, Công an tỉnh đề nghị các sở, ban, ngành thuộc tỉnh; UBND các xã, phường phối hợp triển khai một số nội dung sau:

1. Chỉ đạo bộ phận chuyên môn tiến hành rà soát các hệ thống thông tin nằm trong chức năng, phạm vi quản lý có sử dụng các sản phẩm Fortinet như: FortiSIEM, FortiFone, FortiGate/FortiOS, FortiSwitchManager. Đối chiếu với phiên bản bị ảnh hưởng để xác định nguy cơ tồn tại lỗ hổng bảo mật nêu trên.

2. Tổ chức cập nhật hệ điều hành, phần mềm, firmware theo khuyến nghị của Fortinet để khắc phục các lỗ hổng, ưu tiên các lỗ hổng nghiêm trọng, cụ thể:

- **FortiSIEM**: cập nhật lên các phiên bản đã vá lỗi 7.1.9 / 7.2.7 / 7.3.5 / 7.4.1 hoặc cao hơn;

- **FortiFone**: cập nhật lên các phiên bản đã vá lỗi 3.0.24 / 7.0.2 hoặc cao hơn;

- **FortiOS**: cập nhật lên các phiên bản đã vá lỗi 7.0.18 / 7.2.12 / 7.4.9 / 7.6.4 hoặc cao hơn (theo nhánh đang sử dụng);

- **FortiSwitchManager**: cập nhật lên các phiên bản đã vá lỗi 7.0.6 / 7.2.7 hoặc cao hơn.

3. Trường hợp chưa thể cập nhật ngay, đề nghị thực hiện một số biện pháp giảm thiểu nhằm hạn chế nguy cơ bị khai thác:

- Đối với FortiSIEM: hạn chế/kiểm soát truy cập tới cổng phMonitor (7900); chỉ cho phép truy cập từ các địa chỉ IP quản trị tin cậy.

- Đối với FortiOS/FortiSwitchManager (liên quan đến lỗ hổng CVE-2025-25249): thực hiện khuyến nghị của Fortinet như gỡ "fabric" access trên các interface không cần thiết; chặn truy cập tới capwap daemon; chặn CAPWAP-CONTROL các cổng 5246-5249 trên các interface có dịch vụ "fabric".

4. Thường xuyên kiểm tra, theo dõi nhật ký hệ thống (logs), cảnh báo bất thường liên quan truy cập quản trị, truy cập web portal, truy cập các cổng dịch vụ nêu trên; kịp thời phát hiện, xử lý các dấu hiệu nghi vấn bị tấn công mạng, hạn chế tối đa thiệt hại có thể xảy ra.

5. Thường xuyên phối hợp với Công an tỉnh (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) tiến hành rà quét các điểm yếu kỹ thuật, lỗ hổng bảo mật của các hệ thống thông tin trong chức năng, phạm vi quản lý; kịp thời khắc phục những điểm yếu kỹ thuật, lỗ hổng bảo mật, không để xảy ra tình trạng bị khai thác, tấn công mạng gây ảnh hưởng đến hoạt động bình thường của các hệ thống thông tin.

Quá trình thực hiện nếu gặp khó khăn, vướng mắc, đề nghị trao đổi với

Công an tỉnh (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) để phối hợp, hướng dẫn.

Công an tỉnh thông báo để các cơ quan, đơn vị, địa phương phối hợp thực hiện./.

Nơi nhận:
- Như trên: Thực hiện;
- Đ/c Chủ tịch UBND tỉnh: Báo cáo;
- Đ/c Giám đốc CAT: Báo cáo;
- Phòng PV01: Theo dõi;
- Lưu VT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Đại tá Thăng Quang Huy