

UBND TỈNH TÂY NINH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: /STTTT-TTGSĐH
V/v lỗ hổng bảo mật ảnh hưởng nghiêm trọng
trong phần mềm PAN-OS

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

Tây Ninh, ngày tháng 4 năm 2024

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các cơ quan tham mưu, giúp việc Tỉnh ủy;
- Mặt trận Tổ quốc và các Đoàn thể chính trị - xã hội;
- Các Sở, ban, ngành tỉnh;
- Các đơn vị ngành dọc;
- Các huyện, thị, thành ủy trực thuộc Tỉnh ủy;
- UBND các huyện, thị xã, thành phố;
- UBND các xã, phường, thị trấn.

Thực hiện theo Công văn số 607/CATTT-NCSC của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc cảnh báo lỗ hổng bảo mật ảnh hưởng nghiêm trọng trong phần mềm PAN-OS (**Thông tin chi tiết phụ lục kèm theo**).

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các đơn vị và góp phần đảm bảo an toàn thông tin trên địa bàn tỉnh, Sở Thông tin và Truyền thông đề nghị các đơn vị, địa phương thực hiện gấp các công việc cụ thể như sau:

- Kiểm tra, rà soát các phần mềm PAN-OS đang sử dụng có khả năng bị ảnh hưởng bởi lỗ hổng trên. Thực hiện nâng cấp lên phiên bản mới nhất để tránh nguy cơ bị tấn công
- Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức uy tín về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

Thông tin liên quan đề nghị liên hệ Ông Đào Quang Phúc - Trung tâm Giám sát, điều hành kinh tế, xã hội tập trung; Điện thoại: 0937.117.128.

Trân trọng./.

Nơi nhận:

- Như trên;
- BGĐ Sở (b/c);
- P.CNTTBCVT;
- Lưu: VT, TTGSĐH.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

PHỤ LỤC

THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT

1. Thông tin lỗ hổng bảo mật

- Mô tả:

- Lỗ hổng CVE-2024-3400 (Điểm CVSS: 10) ảnh hưởng trên phần mềm PAN-OS trong gateway GlobalProtect hiện đang bị sử dụng để khai thác. Đối tượng tấn công khai thác lỗ hổng chèn lệnh này có thể thực thi mã từ xa với quyền root trên tường lửa. Lỗ hổng gây ảnh hưởng cho tường lửa cấu hình trên GlobalProtect gateway và telemetry của thiết bị.

- Ảnh hưởng:

- PAN-OS 11.1 trước bản 11.1.2-h3
- PAN-OS 11.0 trước bản 11.0.4-g1
- PAN-OS 10.2 trước bản 10.2.9-h1

- **Đánh giá mức độ:** Lỗ hổng CVE-2024-3400 (Điểm CVSS: 10) ảnh hưởng trên phần mềm PAN-OS trong gateway GlobalProtect. Thông tin về lỗ hổng này chỉ được tiết lộ vài giờ trước, đặt ra một **cảnh báo cấp bách** và yêu cầu các **biện pháp khẩn cấp** để ngăn chặn sự nguy hại từ lỗ hổng này. Việc rà soát và nâng cấp phiên bản hoặc áp dụng biện pháp khắc phục thay thế cần được thực hiện ngay lập tức.

2. Hướng dẫn khắc phục:

Trước mắt, người dùng nên bật Threat ID 95187 và đảm bảo các biện pháp bảo mật lỗ hổng đã được áp dụng cho GlobalProtect. Trong trường hợp không thể bật Threat ID 95187, người dùng nên tạm thời tắt chức năng telemetry trên thiết bị cho tới cập nhật bản vá và chỉ nên bật lại sau khi đã cập nhật bản vá. Các bước để thực hiện việc tắt telemetry như sau:

1. Device > Setup > Telemetry;
2. Chọn widget Telemetry;
3. Bỏ chọn mục “Enable Telemetry”;
4. Bấm OK để lưu thay đổi.

5. Nguồn tham khảo:

<https://security.paloaltonetworks.com/CVE-2024-3400>

<https://www.csa.gov.sg/alerts-advisories/alerts/2024/al-2024-040>