BỘ THÔNG TIN TRUYỀN THÔNG **CỤC AN TOÀN THÔNG TIN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 607 /CATTT-NCSC V/v lỗ hổng bảo mật ảnh hưởng nghiêm trọng trong phần mềm PAN-OS	*Hà Nội, ngày 17 tháng 04 năm 2024*

Kính gửi:

- Đơn vị chuyên trách về CNTT/ATTT các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước;
- Các Doanh nghiệp cung cấp dịch vụ viễn thông, Internet và nền tảng số;
- Các Tổ chức tài chính, Ngân hàng thương mại.
- Hệ thống các đơn vị chuyên trách về an toàn thông tin.

Qua công tác giám sát an toàn không gian mạng quốc gia, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin, ghi nhận mã khai thác của lỗ hổng tồn tại trong phần mềm PAN-OS đã được sử dụng để tấn công vào hệ thống thông tin của nhiều cơ quan, tổ chức.

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.

Thông tin chi tiết lỗ hổng bảo mật xem tại Phụ lục gửi kèm theo.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý Đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Cục An toàn thông tin khuyến nghị Quý Đơn vị thực hiện:

1. 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 (*Tham khảo thông tin tại Phụ lục gửi kèm theo*).

2. 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 lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

3. Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn

thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ais@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Phạm Đức Long (để b/c);
- Cục A05 (Bộ Công an);
- Bộ Tư lệnh 86 (Bộ Quốc phòng);
- Ban Cơ yếu Chính phủ;
- Đơn vị chuyên trách về CNTT/ATTT của: Văn phòng Trung ương Đảng, Văn phòng Quốc hội, Văn phòng Chủ tịch nước, Tòa án nhân dân tối cao, Viện Kiểm sát nhân dân tối cao, Kiểm toán Nhà nước, Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam;
- Các Cục: Viễn thông, Bưu điện Trung ương;
- Trung tâm VNNIC, Trung tâm Thông tin;
- Cục trưởng (để b/c);
- Các Phó Cục trưởng;
- P.ATHTTT, P.QHPT, VNCERT/CC;
- Lưu: VT, NCSC.LTQ.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Trần Đăng Khoa

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG AN TOÀN THÔNG TIN
(Kèm theo Công văn số /CATTT-NCSC ngày / /2024 của Cục An toàn thông tin)

1. Thông tin các 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.

Lỗ hổng này ảnh hưởng đến các phiên bản:

- 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

- Bản vá cho các phiên bản bị ảnh hưởng sẽ được phát hành ngày 14/04/2024, người dùng nên cập nhật ngay khi khả dụng.

Dưới đây là một số IoC được ghi nhận:

- Update.py
- 3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac
- 5460b51da26c060727d128f3b3d6415d1a4c25af6a29fef4cc6b867ad3659078
- 172.233.228[.]93
- hxxp://172.233.228[.]93/policy
- hxxp://172.233.228[.]93/patch
- 66.235.168[.]222

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.

3. Tài liệu tham khảo

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

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