UBND TỈNH KIÊN GIANG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số : 1290 /STTTT-CĐS
V/v cảnh báo lỗ hổng an toàn thông tin CVE-2024-24919 tồn tại trên các sản phẩm của hãng Check Point

Kiên Giang, ngày 06 tháng 6 năm 2024

Kính gửi:
- Văn phòng Tỉnh ủy;
- Văn phòng UBND tỉnh;
- Sở, ban, ngành cấp tỉnh;
- UBND các huyện, thành phố;
- Phòng Văn hóa - Thông tin các huyện, thành phố.

Sở Thông tin và Truyền thông Kiên Giang nhận được Công văn số 995/CATTT-NCSC ngày 31/5/2024 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc cảnh báo lỗ hổng an toàn thông tin CVE-2024-24919 tồn tại trên các sản phẩm của hãng Check Point.

Trong quá trình giám sát an toàn thông tin trên không gian mạng, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), thuộc Cục An toàn thông tin - Bộ Thông tin và Truyền thông, đã phát hiện và ghi nhận các thông tin liên quan đến lỗ hổng an toàn thông tin CVE-2024-24919 tồn tại trên các sản phẩm của hãng Check Point. Lỗ hổng cho phép đối tượng tấn công không cần xác thực đọc nội dung tập tin bất kỳ trên sản phẩm Check Point Security Gateways kết nối tới Internet và đang được thiết lập IPsec VPN Blade nằm trong nhóm Remote Access VPN hoặc Mobile Access Software Blade. Lỗ hổng này hiện đang được khai thác trong môi trường thực tế.

(Thông tin chi tiết xem tại phụ lục kèm theo)

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan, đơn vị trên địa bàn tỉnh, góp phần bảo đảm an toàn cho không gian mạng Việt Nam. Sở Thông tin và Truyền thông Kiên Giang khuyến nghị các cơ quan, đơn vị thực hiện một số biện pháp sau:

1. Kiểm tra, rà soát hệ thống thông tin đang sử dụng có khả năng bị ảnh hưởng bởi chiến dịch tấn công trên. Chủ động theo dõi các thông tin liên quan đến chiến dịch tấn công mạng, sẵn sàng các biện pháp bảo mật để tránh nguy cơ bị tấn công.

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 sau:

- Cục An toàn thông tin - Bộ Thông tin và Truyền thông: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ncsc@ais.gov.vn.

- Hoặc Phòng Chuyển đổi số - Sở Thông tin và Truyền thông Kiên Giang, điện thoại: 0297.3921678.

Trân trọng./.

Nơi nhận:
- Như trên;
- Trung tâm CNTTTT (p/h);
- Lưu: VT, CĐS (ttnghi).

GIÁM ĐỐC

CỘNG HÒA XHCN VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH KIÊN GIANG

Võ Minh Trung

PHỤ LỤC
THÔNG TIN CHI TIẾT VỀ MÃ ĐỘC
(Kèm theo Công văn số 1290 /STTTT-CĐS ngày 06/ 6/2024 của Sở Thông tin và Truyền Thông Kiên Giang)

1. Thông tin chi tiết về lỗ hổng an toàn thông tin trên Check Point

Trung tâm Giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin ghi nhận thông tin liên quan đến lỗ hổng CVE-2024-24919 tồn tại trên các sản phẩm của hãng Check Point. Lỗ hổng cho phép đối tượng tấn công không cần xác thực đọc nội dung tập tin bất kỳ trên sản phẩm Check Point Security Gateways kết nối tới Internet và đang được thiết lập IPsec VPN Blade nằm trong nhóm Remote Access VPN hoặc Mobile Access Software Blade. Lỗ hổng này hiện đang bị khai thác trong môi trường thực tế. Hiện lỗ hổng đã được vá trong bản cập nhật mới nhất của hãng Check Point.

Lỗ hổng là một lỗi Path Traversal ảnh hưởng tới endpoint "/clients/MyCRL" có chức năng trả về nội dung của tập tin trên máy chủ ứng dụng. Endpoint có thể được truy cập thông qua cả hai phương thức GET và POST. Việc khai thác thành công lỗ hổng Path Traversal cho phép đối tượng tấn công đọc nội dung tập tin tùy ý trên hệ thống với đặc quyền cao (root).

2. Tài liệu tham khảo

https://support.checkpoint.com/results/sk/sk182336

https://labs.watchtowr.com/check-point-wrong-check-point-cve-2024-24919/