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: 995 /CATTT-NCSC
V/v cảnh báo lỗ hổng an toàn thông tin CVE-2024-24919 tồn tại trên các sản phẩm của hãng Check Point

Hà Nội, ngày 31 tháng 05 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.

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 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 hệ thống thông tin đang sử dụng có khả năng bị ảnh hưởng bởi lỗ hổng an toàn thông tin trên. Chủ động theo dõi các thông tin liên quan đến lỗ hổng từ hãng nhằm thực hiện nâng cấp lên phiên bản mới nhất 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 của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại: 02432091616, thư điện tử: ncsc@ais.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; 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;
- Ngân hàng Chính sách xã hội;
- Ngân hàng Phát triển Việt Nam;
- Ngân hàng Hợp tác xã Việt Nam;
- Các Tổ chức, doanh nghiệp hoạt động trong lĩnh vực thương mại điện tử;
- Các tổ chức, doanh nghiệp cung cấp dịch vụ trung gian thanh toán, ví điện tử;
- Cục trưởng (để b/c);
- Phó Cục trưởng Trần Đăng Khoa;
- P.ATHTTT, P.QHPT, VNCERT/CC;
- Lưu: VT, NCSC.LTQ.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

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

Trần Đăng Khoa

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

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/