

SỞ THÔNG TIN VÀ TRUYỀN THÔNG CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
TỈNH THANH HÓA
TRUNG TÂM CNTT&TT

Độc lập - Tự do - Hạnh phúc

Số: /TTCNTT&TT-QTHT

Thanh Hoá, ngày tháng năm 2024

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

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các sở, ban, ngành cấp tỉnh;
- UBND các huyện, thị xã, thành phố;
- Các tổ chức đoàn thể chính trị cấp tỉnh;
- Các doanh nghiệp VT, CNTT trên địa bàn tỉnh.

Căn cứ Công văn số 995/CATTT-NCSC ngày 31/05/2024 về việc cảnh báo lỗ hổng an toàn thông tin CVE-2024-24919 tồn tại trên các sản phẩm của hãng Check Point của Cục An toàn thông tin, Bộ Thông tin và Truyền thông. 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)

Để bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin trong các cơ quan nhà nước trên địa bàn tỉnh, Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa đề nghị các cơ quan, đơn vị chỉ đạo các bộ phận, cá nhân thực hiện những nội dung sau:

1. Tổ chức 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. Chỉ đạo Tổ ứng cứu sự cố an toàn thông tin mạng tại cơ quan, địa phương mình triển khai chủ động rà soát và sẵn sàng phương án xử lý sự cố khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời phổ biến, tuyên truyền kịp thời các nguy cơ về mất an toàn thông tin được cảnh báo của các cơ quan chức năng trong phạm vi cơ quan, địa phương.

Trong quá trình thực hiện, nếu gặp khó khăn, vướng mắc về kỹ thuật liên quan đến các nội dung, công việc trên đề nghị liên hệ với Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa để phối hợp hỗ trợ, xử lý.

Điện thoại: (0237)3718.699; Thư điện tử: ungcusuco@thanhhoa.gov.vn./.

Nơi nhận:

- Như kính gửi;
- Sở TT&TT (để b/c);
- PGĐ Sở Nguyễn Văn Tước (để b/c);
- Giám đốc Trung tâm (để b/c);
- Lưu: VT, QTHT.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Trần Ngọc Hưng

Phụ lục

THÔNG TIN CHI TIẾT VỀ LỖ HỔNG 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/>