UBND TỈNH NGHỆ AN
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 1069 /STTTT-CĐS

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

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

Nghệ An, ngày 03 tháng 6 năm 2024

Kính gửi:
- Các Sở, ban, ngành cấp tỉnh;
- UBND các huyện, thành phố, thị xã;
- Viễn thông Nghệ An.

Ngày 31/05/2024, Cục An toàn thông tin đã ban hành công văn số 995/CATTT-NCSC về việc cảnh báo lỗ hổng an toàn thông tin CVE-2024-24919 tồn tại trên các sản phẩm của hãng Check Point. Theo văn bản này, qua theo dõi, giám sát 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*).

Thực hiện chức năng quản lý nhà nước về an toàn thông tin mạng, Sở Thông tin và Truyền thông đề nghị các cơ quan, tổ chức, doanh nghiệp rà soát và triển khai bảo đảm an toàn thông tin mạng cho các hệ thống thông tin thuộc phạm vi quản lý, với các nhiệm vụ chính như sau:

1. Một số giải pháp cần triển khai:

- 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.

- 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.

2. Đề nghị Cổng Thông tin điện tử Nghệ An

a) Đăng tải toàn văn nội dung công văn số 955/CATTT-NCSC ngày 31/05/2024 của Cục An toàn thông tin về việc cảnh báo lỗ hổng an toàn thông tin

CVE-2024-24919 tồn tại trên các sản phẩm của hãng Check Point lên Cổng thông tin điện tử tỉnh Nghệ An.

b) Tham mưu, xây dựng kế hoạch ứng phó các sự cố an toàn thông tin đối với hệ thống thông tin do đơn vị mình được giao quản lý.

c) Tổ chức kiểm tra, rà soát, kịp thời có phương án xử lý đối với các hệ thống hiện đang chủ trì quản trị kỹ thuật.

d) Bố trí cán bộ kỹ thuật thường xuyên theo dõi hệ thống, hỗ trợ người sử dụng khi có nhu cầu.

4. Giao Trung tâm CNTT&TT Nghệ An

a) Tổ chức kiểm tra, rà soát, kịp thời có phương án xử lý đối với các hệ thống hiện đang chủ trì quản trị kỹ thuật, đặc biệt hệ thống mạng máy tính của Sở Thông tin và Truyền thông.

b) Tham mưu, xây dựng kế hoạch ứng phó các sự cố an toàn thông tin, sự cố đối với hệ thống thông tin của tỉnh trình Đội trưởng đội ứng cứu sự cố tỉnh Nghệ An và UBND tỉnh phê duyệt theo thẩm quyền.

c) Bố trí đủ cán bộ thuộc bộ phận ứng cứu sự cố sẵn sàng thực hiện nhiệm vụ khi có điều động.

d) Nghiên cứu giải pháp hỗ trợ các đơn vị khắc phục sự cố khi có yêu cầu.

e) Thường xuyên, liên tục sử dụng các Nền tảng về an toàn thông tin do Cục An toàn thông tin (Bộ Thông tin và Truyền thông) phát triển, cung cấp để hỗ trợ các cơ quan, tổ chức, doanh nghiệp: Sử dụng Nền tảng Điều phối xử lý sự cố an toàn thông tin mạng quốc gia (IRLab) để được hướng dẫn, nhận các cảnh báo sớm và hỗ trợ xử lý sớm nguy cơ, sự cố; Sử dụng Nền tảng Hỗ trợ điều tra số (DFLab) trong trường hợp phù hợp để tổ chức ứng cứu sự cố và được sự hỗ trợ từ cơ quan nhà nước, các chuyên gia đầu ngành về an toàn thông tin.

5. Viễn thông Nghệ An

- Tuân thủ các quy định pháp lý hiện hành và các điều khoản thuộc hợp đồng thuê dịch vụ có liên quan đến công tác an toàn thông tin để đảm bảo hoạt động ổn định, an toàn các hệ thống thông tin hiện đang cung cấp dịch vụ cho tỉnh Nghệ An.

- Khai thác các chức năng của Trung tâm Giám sát an ninh mạng SOC tỉnh Nghệ An để kịp thời cảnh báo, ngăn chặn, hỗ trợ xử lý các sự cố mạng trong các cơ quan nhà nước của tỉnh.

Trong quá trình thực hiện, nếu có khó khăn vướng mắc hoặc trường hợp cần hỗ trợ giám sát, xử lý, ứng cứu sự cố đề nghị liên hệ thông qua các đầu mối:

- Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC), điện thoại 024.3640.4421 hoặc số điện thoại trực đường dây

nóng ứng cứu sự cố 086.9100.317, thư điện tử: ir@vncert.vn;

- Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại: 024.32091.616 hoặc số điện thoại trực đường dây nóng hỗ trợ giám sát, cảnh báo sớm 038.9942.878, thư điện tử: ais@mic.gov.vn.

- Phòng An toàn hệ thống thông tin, Cục An toàn thông tin (hướng dẫn công tác bảo đảm an toàn hệ thống thông tin theo cấp độ), điện thoại: 0369596886, thư điện tử: athttt@mic.gov.vn.

- Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh Nghệ An, điện thoại: 02383.500027.

Trân trọng!./.

Nơi nhận:
- Như trên;
- Cục ATTT, Bộ TT&TT (b/c);
- UBND tỉnh Nghệ An (b/c);
- Ban Giám đốc Sở;
- Cổng TTĐT Nghệ An;
- TrT. CNTT&TT Nghệ An;
- VNPT Nghệ An;
- Lưu: VT, CĐS (đ/c Hợi).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH NGHỆ AN

Võ Trọng Phú

Phụ lục

THÔNG TIN CHI TIẾT VỀ LỖ HỔNG AN TOÀN THÔNG TIN

(Kèm theo Công văn số /STTTT-CĐS ngày 31/05/2024 của Sở Thông tin và Truyền thông)

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/