

ỦY BAN NHÂN DÂN
XÃ HÀNH PHƯỚC

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

Số: /UBND

Hành Phước, ngày 04 tháng 6 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:

- Công an xã, Ban Chỉ huy Quân sự xã;
- Các cơ quan, đơn vị thuộc UBND xã;
- Các cơ quan đóng trên địa bàn xã;
- Cán bộ, công chức và người hoạt động không chuyên trách xã.

Theo cảnh báo của Cục An toàn thông tin tại Công văn số 995/CATTT-NCSC ngày 31/5/2024 và Công văn Số 1101/STTTT-BCVT&CNTT ngày 03/6/2024 của Sở 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; Thực hiện Công văn số 1235/UBND ngày 03/6/2024 của UBND huyện Nghĩa Hành; Chủ tịch UBND xã đề nghị các cơ quan, đơn vị và toàn thể cán bộ, công chức cơ quan thực hiện một số biện pháp sau để hạn chế các rủi ro về nguy cơ mất an toàn thông tin, cụ thể:

1. Kiểm tra, rà soát các hệ thống thông tin có khả năng bị ảnh hưởng bởi lỗ hổng an toàn thông tin CVE-2024-24919 tồn tại trên các sản phẩm của hãng Check Point. 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.

3. Khi phát hiện các hệ thống có biểu hiện bị khai thác, tấn công mạng, triển khai ngay các biện pháp xử lý ngăn chặn tấn công trên hệ thống và thông báo về bộ phận VHXH xã để tổng hợp báo cáo Đội ứng cứu sự cố an toàn thông tin mạng của huyện Nghĩa Hành và tỉnh Quảng Ngãi để có các biện pháp hỗ trợ, xử lý kịp thời.

(Gửi kèm Phụ lục thông tin về lỗ hổng)

Đề nghị các cơ quan, đơn vị, cán bộ, công chức và người hoạt động không chuyên trách xã quan tâm thực hiện./.

Nơi nhận:

- Như trên;
- Phòng VHHT huyện;
- TT Đảng ủy, TT HĐND xã;
- CT, các PCT UBND xã;
- UBMTTQVN xã và các tổ chức CT-XH xã;
- Trang TTĐT xã;
- Lưu: VT.

CHỦ TỊCH

Cao Văn Đạt

PHỤ LỤC
THÔNG TIN CHI TIẾT VỀ LỖ HỔNG AN TOÀN THÔNG TIN
(Kèm theo Công văn số 177/UBND ngày 04/6/2024
của UBND xã Hành Phước)

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/>
