UBND TỈNH ĐỒNG NAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 2422 /STTTT-CĐS
V/v cảnh báo rủi ro an toàn thông tin liên quan đến sản phẩm của CrowdStrike.

Đồng Nai, ngày 22 tháng 7 năm 2024

Kính gửi:
- Các cơ quan Đảng, Nhà nước trên địa bàn tỉnh;
- Ủy ban Mặt trận Tổ quốc Việt Nam tỉnh;
- Các tổ chức chính trị - xã hội trên địa bàn tỉnh;
- Ngân hàng nhà nước tỉnh Đồng Nai;
- Báo Đồng Nai, Đài Phát thanh truyền hình Đồng Nai;
- Các doanh nghiệp Viễn thông: VNPT, Viettel, MobiFone, FPT.

Sở Thông tin và Truyền thông nhận được văn bản số 1384/CATTTT-NCSC ngày 20/7/2024 của Cục An toàn thông tin về việc cảnh báo rủi ro an toàn thông tin liên quan đến sản phẩm của CrowdStrike. Cụ thể:

Các máy tính chạy hệ điều hành Windows 10 và cài đặt phần mềm Falcon Sensor của hãng CrowdStrike đều gặp lỗi màn hình xanh (Blue Screen Of Death - BSOD) và không thể khởi động lại để hoạt động bình thường. Điều này gây ảnh hưởng tới hệ thống thông tin và hoạt động của cá nhân, cơ quan, tổ chức. Nhà phát triển CrowdStrike đã đưa ra thông báo xác nhận rủi ro và thực hiện khôi phục phần mềm Falcon Sensor để tránh gây thêm ảnh hưởng tới thiết bị của người dùng. Thông tin chi tiết và hướng dẫn khắc phục đối với các thiết bị đã bị ảnh hưởng được trình bày tại phụ lục kèm theo văn bản số 1384/CATTTT-NCSC (đính kèm).

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, Sở Thông tin và Truyền thông đề nghị Quý đơn vị nghiên cứu khuyến nghị của Cục An toàn thông tin để thực hiện, đồng thời triển khai đến các đơn vị thuộc phạm vi quản lý các nội dung sau:

1. Kiểm tra, rà soát hệ thống thông tin đang sử dụng có khả năng bị ảnh hưởng bởi rủi ro an toàn thông tin trên. Chủ động theo dõi các thông tin liên quan nhằm thực hiện khắc phục rủi ro trong trường hợp bị ảnh hưởng.

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.

Địa chỉ: Số 01, đường 30/4, phường Thanh Bình, thành phố Biên Hòa, tỉnh Đồng Nai
Số điện thoại: 0251.3810269 – Website: https://stttt.dongnai.gov.vn

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.

Đề nghị Quý đơn vị quan tâm thực hiện./.

Nơi nhận:
- Như trên;
- Ban Giám đốc;
- Phòng VHTT các huyện, TP;
- Lưu: VT, CĐS. Chương

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH ĐỒNG NAI

Võ Hoàng Khai

Phụ lục

THÔNG TIN CHI TIẾT VỀ RỦI RO AN TOÀN THÔNG TIN

(Kèm theo Công văn số 1384/CATTT-NCSC ngày 20/7/2024 của Cục An toàn thông tin)

---

1. Thông tin chi tiết về rủi ro an toàn thông tin liên quan đến sản phẩm của CrowdStrike

Cục An toàn thông tin đã phát hiện rủi ro an toàn thông tin liên quan đến sản phẩm của CrowdStrike. Cụ thể, các máy tính chạy hệ điều hành Windows 10 và cài đặt phần mềm Falcon Sensor của hãng CrowdStrike đều gặp lỗi màn hình xanh (Blue Screen Of Death - BSOD) và không thể khởi động lại để hoạt động bình thường. Điều này gây ảnh hưởng tới hệ thống thông tin và hoạt động của cá nhân, cơ quan, tổ chức. Nhà phát triển CrowdStrike đã đưa ra thông báo xác nhận rủi ro và thực hiện khôi phục phần mềm Falcon Sensor để tránh gây thêm ảnh hưởng tới thiết bị của người dùng.

Hướng dẫn khắc phục đối với các thiết bị đã bị ảnh hưởng:

Bước 1: Khởi động lại máy tính và vào chế độ Safe Mode hoặc Windows Recovery Environment.

Bước 2: Truy cập thư mục "C:\Windows\System32\drivers\CrowdStrike"

Bước 3: Xóa bỏ các tập tin có định dạng "C-00000291*.sys" (tập tin có định dạng .sys và tên bắt đầu bằng chuỗi C-00000291)

Bước 4: Khởi động lại máy tính và sử dụng như bình thường.

2. Tài liệu tham khảo

https://supportportal.crowdstrike.com/s/article/Tech-Alert-Windows-crashes-related-to-Falcon-Sensor-2024-07-19