

Số: _____/STTTT-CNTT

Thành phố Hồ Chí Minh, ngày _____ tháng _____ năm 2024

Về cảnh báo rủi ro an toàn thông tin
liên quan đến sản phẩm của
CrowdStrike

Kính gửi:

- Văn phòng Ủy ban nhân dân Thành phố Hồ Chí Minh;
- Các sở, ban, ngành;
- Trung tâm Chuyển đổi số Thành phố;
- Ủy ban nhân dân thành phố Thủ Đức;
- Ủy ban nhân dân các Quận/huyện;
- Các công ty, tổng công ty trực thuộc Ủy ban nhân dân Thành phố.

Theo thông báo của Cục An toàn thông tin – Bộ Thông tin và Truyền thông, ghi nhận các thông tin liên quan đến sản phẩm của CrowdStrike. Sự cố trên đã gây ảnh hưởng tới nhiều cơ quan, tổ chức trên thế giới, trong đó bao gồm Đức, Singapore, Tây Ban Nha, Ấn Độ, Israel, Nam Phi, 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. *(Đính kèm phụ lục).*

Nhằm bảo đảm an toàn thông tin cho hệ thống thông tin tại các đơn vị, Sở Thông tin và Truyền thông đề nghị các đơn vị triển khai một số nội dung cụ thể như 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.

3. Đầu mối hỗ trợ

Đội ứng cứu sự cố an toàn thông tin mạng thành phố:

- Số điện thoại hotline 24/7: 0889490111.
- Số điện thoại trong giờ hành chính: 38233717 ext: 111.

Thư điện tử: ATTT@tpHCM.gov.vn.

Sở Thông tin và Truyền thông chuyển thông tin đến các đơn vị để biết và khẩn trương thực hiện./.

Nơi nhận:

- Như trên;
- Giám đốc Sở;
- PGĐ Võ Minh Thành;
- Lưu: VT, P.CNTT (TK.110).

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Võ Minh Thành

PHỤ LỤC
THÔNG TIN CHI TIẾT VỀ RỦI RO AN TOÀN THÔNG TIN
(Kèm theo Công văn số /STTTT-CNTT ngày / / 2024
của Sở Thông tin và Truyền thông)

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>