

Số: /VHTT-CNTT

Hà Nội, ngày tháng năm 2024

V/v cảnh báo rủi ro an toàn
thông tin liên quan đến phần mềm
của hãng CrowdStrike

Kính gửi:

- Các cơ quan, đơn vị thuộc huyện;
- UBND các xã, thị trấn.

Thực hiện Văn bản số 2100/STTTT-ATTTGDĐT ngày 23/07/2024 của Sở Thông tin và Truyền thông Hà Nội về việc cảnh báo rủi ro an toàn thông tin liên quan đến phần mềm của hãng CrowdStrike. Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan, đơn vị góp phần bảo đảm an toàn không gian mạng, Phòng Văn hoá và thông tin khuyến nghị 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 (*Thông tin chi tiết xem tại Phụ lục kèm theo*).

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. 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.

Nơi nhận:

- Như trên;
- Lưu VHTT.

**KT. TRƯỞNG PHÒNG
PHÓ TRƯỞNG PHÒNG**

Nguyễn Như Độ

Phụ lục
THÔNG TIN CHI TIẾT VỀ RỦI RO AN TOÀN THÔNG TIN
(Kèm theo Văn bản số /NHTT-CNTT ngày 30/7/2024
của Phòng Văn hoá và Thông tin huyện)

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>