

Số: /STTTT-CNTT

Đắk Lắk, ngày tháng 7 năm 2024

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

Kính gửi:

- Các sở, ban, ngành, đoàn thể của tỉnh;
- UBND các huyện, thị xã, thành phố.

Thực hiện Công văn số 1348/CATTT-NCSC ngày 20/7/2024 của Cục An toàn thông tin, Bộ Thông tin và Truyền thông về việc cảnh báo rủi ro an toàn thông tin liên quan đến sản phẩm của CrowdStrike. Trong quá trình giám sát an toàn thông tin trên không gian mạng, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) thuộc Cục An toàn thông tin đã phát hiện rủi ro an toàn thông tin liên quan đến sản phẩm của CrowdStrike, cụ thể: trên máy tính chạy hệ điều hành Windows 10 có cài đặt phần mềm Falcon Sensor của hãng CrowdStrike gây lỗi màn hình xanh (Blue Screen Of Death - BSOD) và không thể khởi động lại để hoạt động bình thường. Do đó, để đảm bảo hoạt động các trang thiết bị của cá nhân, cơ quan, tổ chức, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị triển khai 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.

3. Thông tin chi tiết về rủi ro an toàn thông tin liên quan đến sản phẩm của CrowdStrike và biện pháp khắc phục đề nghị các cơ quan, đơn vị tham khảo tại *Phụ lục kèm theo*.

4. Trong trường hợp cần thiết liên hệ về 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.

Nhận được Công văn này, Sở Thông tin và Truyền thông kính đề nghị các cơ quan, đơn vị quan tâm, triển khai thực hiện./.

Nơi nhận:

- Như trên;
- UBND tỉnh (b/c);
- Cục An toàn thông tin (b/c);
- Lãnh đạo Sở;
- ĐAKLAKIOC (t/h);
- Lưu: VT, CNTT.

GIÁM ĐỐC

Trương Hoài Anh

Phụ lục
THÔNG TIN CHI TIẾT VÀ BIỆN PHÁP KHẮC PHỤC LIÊN QUAN
ĐẾN SẢN PHẨM CỦA CROWDSTRIKE

(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.

2. 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.

3. Tài liệu tham khảo

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