BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Số: 392 /TTCNTT-HTATTT
V/v cảnh báo rủi ro an toàn thông tin liên quan đến sản phẩm của CrowdStrike

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

Hà Nội, ngày 24 tháng 07 năm 2024

Kính gửi: Các đơn vị trực thuộc Bộ
(Danh sách kèm theo)

Ngày 20/07/2024 Cục An toàn thông tin – Bộ Thông tin và Truyền thông đã phát hành Công văn số 1384/CATTT-NCSC về việc cảnh báo rủi ro an toàn 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. Thông tin chi tiết và hướng dẫn khắc phục đối với các thiết bị đã bị ảnh hưởng được trình bày tại Phụ lục.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý Đơn vị và người sử dụng, Trung tâm Công nghệ thông tin khuyến nghị Quý Đơn vị thực hiện:

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.

Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Trung tâm Công nghệ thông tin: Phòng Hạ tầng và an toàn thông tin, 113 Trần Duy Hưng, Trung Hòa, Cầu Giấy, Hà Nội; số điện thoại: 024.39439060; địa chỉ thư điện tử: phongktht@most.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Bùi Thế Duy (để b/c);
- Giám đốc (để b/c);
- Cổng thông tin điện tử của Bộ (để đăng tải);
- Lưu: VT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Ngô Minh Phước

Phụ lục
THÔNG TIN CHI TIẾT VỀ RỦI RO AN TOÀN THÔNG TIN
(Kèm theo Công văn số 392 /TTCNTT-HTATTT ngày24 / 07 /2024 của Trung tâm Công nghệ 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

DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN

(Kèm theo Công văn số 392 /TTCNTT-HTATTT ngày 24 /07/2024 của Trung tâm Công nghệ thông tin)

TT	Tên đơn vị
1.	Thanh tra Bộ
2.	Cục Phát triển công nghệ và Đổi mới sáng tạo.
3.	Cục Thông tin khoa học và công nghệ quốc gia
4.	Cục Phát triển thị trường và doanh nghiệp khoa học và công nghệ
5.	Cục An toàn bức xạ và hạt nhân
6.	Cục Sở hữu trí tuệ
7.	Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia
8.	Học viện Khoa học, Công nghệ và Đổi mới sáng tạo
9.	Viện Khoa học và công nghệ Việt Nam - Hàn Quốc (VKIST)
10.	Viện Nghiên cứu sáng chế và Khai thác công nghệ
11.	Viện Năng lượng nguyên tử Việt Nam
12.	Viện Ứng dụng công nghệ
13.	Viện Đánh giá khoa học và Định giá công nghệ
14.	Viện Khoa học sở hữu trí tuệ
15.	Viện Nghiên cứu và Phát triển Vùng
16.	Văn phòng các Chương trình trọng điểm cấp nhà nước
17.	Văn phòng Công nhận chất lượng
18.	Văn phòng Đăng ký hoạt động khoa học và công nghệ
19.	Văn phòng các Chương trình khoa học và công nghệ quốc gia
20.	Báo VnExpress
21.	Tạp chí Khoa học và Công nghệ Việt Nam
22.	Nhà xuất bản Khoa học và Kỹ thuật
23.	Quỹ Phát triển khoa học và công nghệ quốc gia
24.	Quỹ Đổi mới công nghệ quốc gia
25.	Trung tâm Nghiên cứu và Phát triển truyền thông khoa học và công nghệ
26.	Trung tâm Nghiên cứu và Phát triển hội nhập khoa học và công nghệ quốc tế
27.	Trung tâm Công nghệ thông tin