UBND TỈNH THANH HOÁ
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG

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

Số: 6882 /STNMT-DLTT

Thanh Hoá, ngày 31 tháng 7 năm 2024

V/v cảnh báo rủi ro an toàn thông tin liên quan đến sản phẩm của CrowdStrike.

Kính gửi: Trưởng các đơn vị thuộc Sở

Sở Tài nguyên và Môi trường nhận được Công văn số 221/TTCNTT&TT-QTHT ngày 27/7/2024 của Trung tâm Công nghệ thông tin và Truyền thông về việc cảnh báo cảnh báo rủi ro an toàn thông tin liên quan đến sản phẩm của CrowdStrike. Căn cứ các Công văn cảnh báo an toàn thông tin của Cục An toàn thông tin, Bộ Thông tin và Truyền thông và qua công tác giám sát an toàn thông tin mạng, đã phát hiện 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 xem tại Phụ lục kèm theo)

Để bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin tại các hệ thống thông tin và máy tính của các đơn vị, Giám đốc Sở có ý kiến chỉ đạo như sau:

1. Giao Trưởng các đơn vị trực thuộc Sở chỉ đạo các bộ phận, cá nhân thực hiện:

- Chủ động tổ chức kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng bởi rủi ro an toàn thông tin trên*(nếu có)*. Chủ động theo dõi các thông tin liên quan nhằm thực hiện khắc phục rủi ro trong trường hợp bị ảnh hưởng.

- Trong quá trình thực hiện, nếu gặp khó khăn, vướng mắc về kỹ thuật liên quan đến các nội dung, công việc liên hệ với Tổ ứng cứu sự cố An toàn thông tin mạng Sở Tài nguyên và Môi trường hoặc Trung tâm Dữ liệu thông tin tài nguyên và môi trường (đơn vị phụ trách an toàn thông tin mạng của Sở trực tiếp theo dõi, chỉ đạo hoạt động của Tổ ứng cứu sự cố).

2. Giao Trung tâm Dữ liệu thông tin tài nguyên và môi trường:

- 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.

- Phối hợp Tổ ứng cứu sự cố Sở, tổ chức tiến hành kiểm tra, rà soát và sẵn sàng phương án xử lý sự cố khi phát hiện có dấu hiệu bị khai thác, tấn công mạng, xử lý, ngăn chặn sự cố mất an toàn thông tin nếu có tại Cơ quan Sở và các đơn vị trực thuộc Sở Tài nguyên và Môi trường.

- Đăng tải hướng dẫn kỹ thuật cách thức thực hiện chi tiết rủi ro an toàn thông tin liên quan đến sản phẩm của CrowdStrike lên Cổng thông tin điện tử của Sở.

Theo các nội dung trên, yêu cầu các đơn vị nghiêm túc triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Giám đốc Sở (để b/c);
- Cổng thông tin điện tử Sở;
- Lưu: VT, TTDLTTTNMT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG
TỈNH THANH HÓA

Nguyễn Khánh Toàn

Phụ lục

THÔNG TIN CHI TIẾT VỀ RỦI RO 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-Windowscrashes-related-to-Falcon-Sensor-2024-07-19