BỘ GIAO THÔNG VẬN TẢI
CỤC HÀNG HẢI VIỆT NAM

Số: 3556 /CHHVN-KHCNMT
V/v cảnh báo các lỗ hổng bảo mật tháng 7 năm 2024.

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

Hà Nội, ngày 31 tháng 7 năm 2024

Kính gửi:
- Các đơn vị trực thuộc.
- Công ty TNHH MTV Thông tin điện tử hàng hải Việt Nam.

Cục Hàng hải Việt Nam nhận được thông tin cảnh báo từ các cơ quan chức năng về rủi ro an toàn thông tin liên quan đến sản phẩm của Microsoft (Windows Remote Desktop Licensing Service, Windows Imaging Component, SharePoint Server, Office, Windows Hyper-V, Windows MSHTML Platform) và CrowdStrike:

- Các lỗ hổng bảo mật liên quan đến sản phẩm của Microsoft cho phép đối tượng tấn công thực thi mã từ xa.

- Sự cố liên quan đến sản phẩm của CrowdStrike 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.

Để bảo đảm an toàn thông tin, an ninh mạng cho Hệ thống công nghệ thông tin của Cục Hàng hải Việt Nam và các đơn vị trực thuộc, Cục Hàng hải Việt Nam yêu cầu Công ty TNHH MTV Thông tin điện tử hàng hải Việt Nam và các đơn vị trực thuộc chủ động thực hiện các biện pháp sau:

1. Kiểm tra, rà soát hệ thống thông tin đang sử dụng có khả năng bị ảnh hưởng bởi các mã độc và 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.

Trường hợp cần thiết, liên hệ với Trung tâm Công nghệ thông tin - Bộ Giao thông vận tải (*ông Dương Đình Trung - số điện thoại 0985366388*) và các cơ quan chức năng về an toàn, an ninh mạng để được hỗ trợ xử lý.

(Thông tin chi tiết và hướng dẫn khắc phục đối với các thiết bị đã bị ảnh hưởng được trình bày tại phụ lục kèm theo).

Cục Hàng hải Việt Nam yêu cầu các đơn vị triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Cục trưởng (*để b/c*);
- Lưu: VT, KHCNMT.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

BỘ GIAO THÔNG VẬN TẢI
CỤC HÀNG HẢI VIỆT NAM

Nguyễn Hoàng

Phụ lục 1

THÔNG TIN VỀ CÁC LỖ HỔNG AN TOÀN THÔNG TIN TRONG SẢN PHẨM MICROSOFT

1. Thông tin các lỗ hổng an toàn thông tin

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-38074 CVE-2024-38076 CVE-2024-38077	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Remote Desktop Licensing Service cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38074 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38076 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38077
2	CVE-2024-38060	- Điểm CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Imaging Component cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38060
3	CVE-2024-38023 CVE-2024-38024 CVE-2024-38094	- Điểm CVSS: 7.2 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, Microsoft SharePoint Server Subscription Edition.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38023 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38024 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38094
4	CVE-2024-38021	- Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office 2016, 2019, Microsoft Office LTSC 2021, Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38021

5	CVE-2024-38080	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 11, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38080
6	CVE-2024-38112	- Điểm CVSS: 7.5 (Cao) - Mô tả: Lỗ hổng trong Windows MSHTML Platform cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng an toàn thông tin nói trên theo hướng dẫn của hãng. Quý đơn vị tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại link nguồn tham khảo tại mục 1 của Phụ lục.

3. Tài liệu tham khảo

https://msrc.microsoft.com/update-guide/

https://www.zerodayinitiative.com/blog/2024/7/9/the-july-2024-security-update-review

Phụ lục 2

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

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