BỘ GIAO THÔNG VẬN TẢI
CỤC HÀNG HẢI VIỆT NAM

Số: 4723 /CHHVN-KHCNMT
V/v cảnh báo lỗ hổng bảo mật.

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

Hà Nội, ngày 09 tháng 10 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 (Microsoft Office and Components, Windows Hyper-V, Windows DHCP Server, Microsoft Streaming Service, Microsoft Management Console, Windows MSHTML Platform, Microsoft Dynamics 365 (on-premise),…). Các lỗ hổng bảo mật này cho phép đối tượng tấn công thực thi mã từ xa. *(Thông tin chi tiết tại phụ lục kèm theo)*.

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, xác định các hệ thống thông tin có khả năng bị ảnh hưởng bởi các mã độc nêu trên. Chủ động theo dõi các thông tin liên quan đến mã độc từ hãng để thực hiện nâng cấp lên phiên bản mới nhất nhằm tránh nguy cơ bị tấn công.

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 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 thông tin, an ninh mạng để được hỗ trợ xử lý.

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 BẢO MẬT TRONG SẢN PHẨM MICROSOFT

1. Thông tin các lỗ hổng

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-43491	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft Windows Update cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43491
2	CVE-2024-38018 CVE-2024-38227 CVE-2024-38228 CVE-2024-43464	- Điểm CVSS: 8.8 (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-2024-38018 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38227 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38228 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43464
3	CVE-2024-43461	- Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Windows MSHTML Platform cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43461
4	CVE-2024-21416 CVE-2024-38045	- Điểm CVSS: 8.1 (Cao) - Mô tả: Lỗ hổng trong Windows TCP/IP cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21416 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38045
5	CVE-2024-38014	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Windows Installer 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 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38014

STT	CVE	Mô tả	Link tham khảo
6	CVE-2024-43463	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office Visio cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Visio 2016, Microsoft Office LTSC 2021, Microsoft 365 Apps for Enterprise, Microsoft Office 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43463
7	CVE-2024-38226	- Điểm CVSS: 7.3 (Cao) - Mô tả: Lỗ hổng trong Microsoft Publisher cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft Publisher 2016, Microsoft Office LTSC 2021, Microsoft Office 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38226
8	CVE-2024-38217 CVE-2024-43487	- Điểm CVSS: 5.4 (Cao) - Mô tả: Lỗ hổng trong Windows Mark of the Web cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. 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-2024-38217 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43487

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/2024/9/10/the-september-2024-security-update-review