BỘ GIAO THÔNG VẬN TẢI
CỤC HÀNG HẢI VIỆT NAM

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

Số: 39 /CHHVN-KHCNMT
V/v cảnh báo lỗ hổng bảo mật.

Hà Nội, ngày 06 tháng 01 năm 2025

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 và các thành phần của Windows, Office và các thành phần của Office, SharePoint Server, Hyper-V, Defender cho Endpoint, System Center Operations Manager. 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 hệ thống thông tin đang sử dụng có khả năng bị ảnh hưởng bởi các lỗ hổng an toàn thông tin nêu trên. Chủ động theo dõi các thông tin liên quan đến các chiến dịch tấn công mạng để thực hiện ngăn chặn 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*), Phòng Khoa học - Công nghệ và Môi trường, Cục Hàng hải Việt Nam *(ông Bùi Ngọc Thi - số điện thoại 0374596606)* 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

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-2024-49138	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Windows Common Log File System Driver 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, 2025.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49138
2	CVE-2024-49112 CVE-2024-49127	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Lightweight Directory Access Protocol (LDAP) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022, 2025.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49112 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49127
3	CVE-2024-49117	- Điểm CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2022, 2025.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49117
4	CVE-2024-49124	- Điểm CVSS: 8.1 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Lightweight Directory Access Protocol (LDAP) Client cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022, 2025.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49124
5	CVE-2024-49126	- Điểm CVSS: 8.1 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Local Security Authority Subsystem Service (LSASS) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022, 2025.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49126

STT	CVE	Mô tả	Link tham khảo
6	CVE-2024-49070	- Điểm CVSS: 7.4 (Cao) - Mô tả: Lỗ hổng trong Microsoft SharePoint cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49070
7	CVE-2024-49068	- Điểm CVSS: 8.2 (Cao) - Mô tả: Lỗ hổng trong Microsoft SharePoint cho phép đối tượng tấn công thực hiện leo thang đặc quyền. - Ảnh hưởng: Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49068
8	CVE-2024-49142	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Access cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Access 2016, Microsoft Office LTSC 2021, 2024, Microsoft 365 Apps for Enterprise, Microsoft Office 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49142
9	CVE-2024-49069	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Excel 2016, Microsoft Office LTSC 2021, 2024, Microsoft 365 Apps for Enterprise, Microsoft Office 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49069
10	CVE-2024-49065	- Điểm CVSS: 5.5 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Word 2016, Microsoft Office LTSC 2021, 2024, Microsoft 365 Apps for Enterprise, Microsoft Office 2019, Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49065

2. Hướng dẫn khắc phục

- Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng.

- 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.

- Kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. 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.

3. Tài liệu tham khảo

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

https://www.zerodayinitiative.com/blog/2024/12/10/the-december-2024-security-update-review