

**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: /CHHVN-KHCNMT
V/v cảnh báo các lỗ hổng bảo mật tháng
10 năm 2023.

Hà Nội, ngày tháng năm 2023

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 về nguy cơ tấn công mạng liên quan tới các lỗ hổng bảo mật trong các sản phẩm của Microsoft (*Exchange Server, WordPad, Skype for Business, Message Queuing, Windows IIS Server*). Các lỗ hổng bảo mật này cho phép đối tượng tấn công thực thi mã từ xa.

Để bảo đảm an toàn thông tin 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 và xác định máy tính, máy chủ sử dụng Hệ điều hành Windows có khả năng bị tấn công theo danh sách các lỗ hổng bảo mật tại Phụ lục gửi kèm theo. Thực hiện cập nhật bản vá kịp thời để 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 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.

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**

Nguyễn Hoàng

PHỤ LỤC

Thông tin về các lỗ hổng bảo mật trong sản phẩm của Microsoft

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-36778	<ul style="list-style-type: none">- Điểm: CVSS: 8.0 (Cao)- Mô tả: Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.- Ảnh hưởng: Microsoft Exchange Server 2016, 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36778
2	CVE-2023-36563	<ul style="list-style-type: none">- Điểm: CVSS: 6.5 (Cao)- Mô tả: Lỗ hổng trong Microsoft WordPad cho phép đối tượng tấn công thực hiện thu thập thông tin mã băm NTLM của người dùng. 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-2023-36563
3	CVE-2023-41763	<ul style="list-style-type: none">- Điểm: CVSS: 5.3 (Cao)- Mô tả: Lỗ hổng trong Skype for Business cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.- Ảnh hưởng: Skype for Business 2015, 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-41763
4	CVE-2023-35349 CVE-2023-36697	<ul style="list-style-type: none">- Điểm: CVSS: 9.8 (Nghiêm trọng)- Mô tả: Lỗ hổng trong Microsoft Message Queuing 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-2023-35349 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36697
5	CVE-2023-36434	<ul style="list-style-type: none">- Điểm: CVSS: 9.8 (Cao)- Mô tả: Lỗ hổng trong Windows IIS Server cho phép đối tượng tấn công thực hiện leo thang đặc quyền.- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36434

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng bảo mật

nêu trên theo hướng dẫn của hãng. Các đơn vị tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại link nguồn tham khảo của phụ lục.

3. Tài liệu tham khảo

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

<https://www.zerodayinitiative.com/blog/2023/10/10/the-october-2023-security-update-review>