BỘ GIAO THÔNG VẬN TẢI
CỤC HÀNG HẢI VIỆT NAM

Số: 633 /CHHVN-KHCNMT
V/v cảnh báo lỗ hổng bảo mật tháng 02 năm 2025.

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

Hà Nội, ngày 18 tháng 02 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 về nguy cơ tấn công mạng liên quan tới các lỗ hổng bảo mật trong các sản phẩm của Microsoft (*Windows và các thành phần của Windows, Office và các thành phần của Office, Hyper-V, SharePoint Server, .NET và Visual Studio, Azure, BitLocker, Remote Desktop Services và Windows Virtual Trusted Platform Module*) và các sản phẩm khác (*Palo Alto Networks PAN-OS, Mitel MiCollab, Router hãng Four-Faith mẫu F3x24 và F3x36, Cleo Harmony, VLTrader, LexiCom, Apache MINA, Apache Struts, Apache Tomcat, FortiClientEMS, ColdFusion*). 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 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; và thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công. 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, an ninh mạng 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

Nguyễn Hoàng

Phụ lục

THÔNG TIN VỀ CÁC LỖ HỔNG AN TOÀN THÔNG TIN

1. Thông tin các lỗ hổng

STT	CVE	Mô tả	Link tham khảo
1	CVE-2025-21333 CVE-2025-21334 CVE-2025-21335	- Điểm CVSS: 7.8 (Cao). - Mô tả: Lỗ hổng trong Windows Hyper-V NT Kernel Integration VSP 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 2025.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21333 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21334 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21335
2	CVE-2025-21298	- Điểm CVSS: 9.8 (Nghiêm trọng). - Mô tả: Lỗ hổng trong Windows OLE 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-2025-21298
3	CVE-2025-21297 CVE-2025-21309	- Điểm CVSS: 8.1 (Nghiêm trọng). - Mô tả: Lỗ hổng trong Windows Remote Desktop Services cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server 2012, 2016, 2019, 2022, 2025.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21297 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21309
4	CVE-2025-21308	- Điểm CVSS: 6.5 (Cao). - Mô tả: Lỗ hổng trong Windows Themes cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). Thông tin chi tiết về lỗ hổng đã được công bố công khai. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2012, 2016, 2019, 2022, 2025.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21308
5	CVE-2025-21186 CVE-2025-21366 CVE-2025-21395	- Điểm CVSS: 7.8 (Cao). - Mô tả: Lỗ hổng trong Microsoft Access cho phép đối tượng tấn công thực thi mã từ xa. Thông tin chi tiết về lỗ hổng đã được công bố công khai. - 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-2025-21186 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21366 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21395

STT	CVE	Mô tả	Link tham khảo
6	CVE-2025-21275	- Điểm CVSS: 7.8 (Cao). - Mô tả: Lỗ hổng trong Windows App Package Installer cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Thông tin chi tiết về lỗ hổng đã được công bố công khai. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2022, 2025.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21275
7	CVE-2025-21311	- Điểm CVSS: 9.8 (Nghiêm trọng). - Mô tả: Lỗ hổng trong Windows NTLM V1 cho phép đối tượng tấn công thực hiện leo thang đặc quyền. - Ảnh hưởng: Windows 11, Windows Server 2022, 2025.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21311
8	CVE-2025-21354 CVE-2025-21362	- 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 Office LTSC 2021, 2024, Microsoft 365 Apps for Enterprise, Microsoft Office 2019, Office Online Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21354 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21362
9	CVE-2025-21402	- Điểm CVSS: 7.8 (Cao). - Mô tả: Lỗ hổng trong Microsoft Office OneNote cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office LTSC 2021, 2024, Microsoft OneNote.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21402
10	CVE-2025-21365	- Điểm CVSS: 7.8 (Cao). - Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office LTSC 2024, Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21365
11	CVE-2025-21345 CVE-2025-21356	- 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 Office LTSC 2021, 2024, Microsoft 365 Apps for Enterprise, Microsoft Office 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21345
12	CVE-2025-21363	- Điểm CVSS: 7.8 (Cao). - Mô tả: Lỗ hổng trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office LTSC 2021, 2024, Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21363

STT	CVE	Mô tả	Link tham khảo
13	CVE-2025-21357 CVE-2025-21361	- Điểm CVSS: 7.8 (Cao). - Mô tả: Lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office LTSC 2021, 2024, Microsoft 365 Apps for Enterprise, Microsoft Office 2019, Microsoft Outlook 2016.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21357 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21361
14	CVE-2025-21344 CVE-2025-21348	- Điểm CVSS: 7.8 (Cao). - Mô tả: Lỗ hổng trong SharePoint Server 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-2025-21344 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21348
15	CVE-2024-3393	- Điểm CVSS: Chưa xác định. - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ. - Ảnh hưởng: Palo Alto Networks PAN-OS. - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-3393
16	CVE-2024-41713	- Điểm CVSS: 7.5 (Cao). - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: Mitel MiCollab. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-41713
17	CVE-2024-12856	- Điểm CVSS: 7.2 (Cao). - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Router hãng Four-Faith mẫu F3x24 và F3x36. - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-12856
18	CVE-2018-0802	- Điểm CVSS: 7.8 (Cao). - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office 2007, 2010, 2016. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2018-0802

STT	CVE	Mô tả	Link tham khảo
19	CVE-2024-49138	- Điểm CVSS: 7.8 (Cao). - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Microsoft Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022, 2025. - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-49138
20	CVE-2024-50623	- Điểm CVSS: 9.8 (Nghiêm trọng). - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Cleo Harmony, VLTrader, LexiCom. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-50623
21	CVE-2024-52046	- Điểm CVSS: 10.0 (Nghiêm trọng). - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Apache MINA. - Lỗ hổng chưa có mã khai thác và chưa bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-52046
22	CVE-2024-53677	- Điểm CVSS: 9.5 (Nghiêm trọng). - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Apache Struts. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-53677
23	CVE-2024-56337	- Điểm CVSS: Chưa xác định. - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Ảnh hưởng: Apache Tomcat. - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-56337
24	CVE-2023-48788	- Điểm CVSS: 9.8 (Nghiêm trọng). - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: FortiClientEMS. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2023-48788
25	CVE-2024-35250	- Điểm CVSS: 7.8 (Cao). - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền.	https://nvd.nist.gov/vuln/detail/CVE-2024-35250

STT	CVE	Mô tả	Link tham khảo
		- Ảnh hưởng: Microsoft Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	
26	CVE-2024-20767	- Điểm CVSS: 7.4 (Cao). - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: ColdFusion. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-20767

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, an ninh mạng 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 nêu trên theo hướng dẫn của hãng.

3. Tài liệu tham khảo

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

https://www.zerodayinitiative.com/blog/2025/1/14/the-january-2025-security-update-review