BỘ GIAO THÔNG VẬN TẢI
**CỤC HÀNG HẢI VIỆT NAM**

Số: 4369 /CHHVN-KHCNMT
V/v cảnh báo các lỗ hổng bảo mật.

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

*Hà Nội, ngày 29 tháng 11 năm 2022*

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 (*Microsoft Exchange Server, Windows Scripting Languages, Windows Mark of the Web, Windows Print Spooler, Windows CNG Key Insolation Service, Windows Point-to-Point, Microsoft Excel*). 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 ảnh hưởng 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**

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 của Microsoft

### 1. Thông tin các lỗ hổng bảo mật

| STT | CVE | Mô tả | Link tham khảo |
|---|---|---|---|
| 1 | CVE-2022-41082, CVE-2022-41040, CVE-2022-41080, CVE-2022-41079, CVE-2022-41078, CVE-2022-41123 | - Điểm CVSS: 8.8 (Cao)<br>- Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa, nâng cao đặc quyền.<br>- Ảnh hưởng: Microsoft Exchange Server 2016 CU 23/22, Exchange Server 2019 CU 11, Exchange Server 2013 CU 23 | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41082<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41080<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41123<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41078<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41079 |
| 2 | CVE-2022-41128, CVE-2022-41118 | - Điểm CVSS: 8.8 (Cao)<br>- Lỗ hổng trong trong Windows Scripting Languages cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đang bị khai thác trong thực tế.<br>- Ảnh hưởng: Windows Server 2008/2012/2016/2019 /2022, Windows 11/10/8.1/7. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41128<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41118 |
| 3 | CVE-2022-41091 | - Điểm CVSS: 5.4 (Trung bình)<br>- Lỗ hổng trong Windows Mark of the Web cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật.<br>- Ảnh hưởng: Windows 10/11, Windows Server 2016/2019/2022. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41091 |
| 4 | CVE-2022-41073 | - Điểm CVSS: 7.8 (Cao)<br>- Lỗ hổng Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền.<br>- Ảnh hưởng: Windows Server 2008/2012/2016/2019 /2022, Windows 11/10/8.1/7. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41073 |
| 5 | CVE-2022-41125 | - Điểm CVSS: 7.8 (Cao)<br>- Lỗ hổng Windows CNG Key Insolation Service cho phép đối | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41125 |

| | | | |
|---|---|---|---|
| | | tượng tấn công thực hiện tấn công nâng cao đặc quyền.<br>- Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019/2022 | |
| 6 | CVE-2022-41044, CVE-2022-41088, CVE-2022-41039 | - Điểm CVSS: 8.1 (Cao)<br>- Lỗ hổng trong Windows Point-to-Point cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41044<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41088<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41039 |
| 7 | CVE-2022-41105, CVE-2022-41106, CVE-2022-41063, CVE-2022-41104 | - Điểm CVSS: 7.8 (Cao)<br>- Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa, tấn công giả mạo (Spoofing), thực hiện tấn công vượt qua cơ chế bảo mật.<br>- Ảnh hưởng: Microsoft Excel 2013/2016, Microsoft Office, Microsoft 365. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41105<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41106<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41063<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41104 |

## 2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng bảo mật nói 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/releaseNote/2022-Nov

https://www.zerodayinitiative.com/blog/2022/11/8/the-november-2022-security-update-review