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

Số: 3007 /CHHVN-KHCNMT
V/v cảnh báo các lỗ hổng bảo mật tháng 7 năm 2023.

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

*Hà Nội, ngày 19 tháng 7 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 (*Microsoft Exchange Server, Microsoft SharePoint Server, Windows Pragmatic General Multicast (PGM), JavaScript V8, Microsoft Excel, Microsoft Office*). 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**

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-2023-32031<br>CVE-2023-28310 | - Điểm: CVSS: 8.8 (Cao)<br>- Mô tả: lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Microsoft Exchange Server 2016, 2019. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32031<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28310 |
| 2 | CVE-2023-29357<br>CVE-2023-33142 | - Điểm: CVSS: 9.8 (Nghiêm trọng)<br>- Mô tả: lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.<br>- Ảnh hưởng: Microsoft SharePoint Server 2019. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29357<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33142 |
| 3 | CVE-2023-29363<br>CVE-2023-32014<br>CVE-2023-32015 | - Điểm: CVSS: 9.8 (Nghiêm trọng)<br>- Mô tả: lỗ hổng trong Windows Pragmatic General Multicast (PGM) cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Windows Server, Windows 10/11. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29363<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32014<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32015 |
| 4 | CVE-2023-3079 | - Điểm: CVSS: N/A<br>- Mô tả: lỗ hổng trong JavaScript V8 cho phép đối tượng tấn công có thể thực thi các đoạn mã với quyền của người dùng cục bộ. Lỗ hổng này đang bị khai thác trong thực tế.<br>- Ảnh hưởng: Microsoft Edge (Chromium-based) | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-3079 |
| 5 | CVE-2023-32029<br>CVE-2023-33133<br>CVE-2023-33137 | - Điểm: CVSS: 7.8 (Cao)<br>- Mô tả: lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Microsoft Excel, Microsoft Office. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32029<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33133<br>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33137 |

| STT | CVE | Mô tả | Link tham khảo |
|---|---|---|---|
| 6 | CVE-2023-33146 | - Điểm: CVSS: 7.8 (cao)<br>- Mô tả: lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.<br>- Ảnh hưởng: Microsoft Office, Microsoft 365. | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33146 |

**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/2023/6/13/the-june-2023-security-update-review