

Số: /STTTT-CNTT&BCVT  
V/v lỗ hổng an toàn thông tin ảnh hưởng cao và  
nghiêm trọng trong các sản phẩm Microsoft  
công bố tháng 06/2024

Tuyên Quang, ngày tháng 6 năm 2024

Kính gửi:

- Văn phòng Đoàn Đại biểu Quốc hội và Hội đồng nhân dân;
- Văn phòng Ủy ban nhân dân tỉnh;
- Các sở, ban, ngành;
- Ủy ban nhân dân các huyện, thành phố.

Căn cứ văn bản số 1096/CATTT-NCSC ngày 14/6/2024 của Cục An toàn thông tin về việc lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 06/2024, Sở Thông tin và Truyền thông cung cấp thông tin và đưa ra các giải pháp phòng, tránh khai thác lỗ hổng bảo mật cao và nghiêm trọng trong các sản phẩm Microsoft như sau:

### **I. Thông tin về lỗ hổng bảo mật trong các sản phẩm Microsoft**

Ngày 11/06/2024, Microsoft đã phát hành danh sách bản vá tháng 06 với 49 lỗ hổng an toàn thông tin trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý vào các lỗ hổng an toàn thông tin có mức ảnh hưởng cao và nghiêm trọng sau:

- Lỗ hổng an toàn thông tin **CVE-2024-30080** trong Microsoft Message Queuing (MSMQ) cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng an toàn thông tin **CVE-2024-30103** trong Microsoft Outlook cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng an toàn thông tin **CVE-2024-30078** trong Windows Wi-Fi Driver cho phép đối tượng tấn công thực thi mã từ xa.
- 03 lỗ hổng an toàn thông tin **CVE-2024-30101, CVE-2024-30102, CVE-2024-30104** trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng an toàn thông tin **CVE-2024-30100** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

*Thông tin chi tiết các lỗ hổng an toàn thông tin xem tại Phụ lục kèm theo.*

### **II. Các giải pháp phòng tránh**

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, góp phần bảo đảm an toàn không gian mạng Việt Nam, Sở Thông tin và Truyền thông

khuyến nghị Quý đơn vị thực hiện:

1. Kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công (tham khảo thông tin tại Phụ lục kèm theo).

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 lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

3. Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại: 02432091616, thư điện tử: [ncsc@ais.gov.vn](mailto:ncsc@ais.gov.vn).

Trân trọng./.

***Nơi nhận:***

- Như trên;
- Ban Giám đốc sở (báo cáo);
- Các đơn vị thuộc Sở;
- Lưu: VT, CNTT&BCVT

**KT. GIÁM ĐỐC  
PHÓ GIÁM ĐỐC**

**Nguyễn Văn Hiến**

**Phụ lục**  
**THÔNG TIN VỀ CÁC LỖ HỔNG AN TOÀN THÔNG TIN**  
**TRONG SẢN PHẨM MICROSOFT**  
*(Kèm theo Công văn số /STTTT-CNTT&BCVT ngày /6/2024*  
*của Sở Thông tin và Truyền thông)*

**1. Thông tin các lỗ hổng an toàn thông tin**

<b>STT</b>	<b>CVE</b>	<b>Mô tả</b>	<b>Link tham khảo</b>
1	CVE-2024-30080	<ul style="list-style-type: none"> <li>- Điểm CVSS: 9.8 (Nghiêm trọng)</li> <li>- Mô tả: Lỗ hổng trong Microsoft Message Queuing (MSMQ) cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30080">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30080</a>
2	CVE-2024-30103	<ul style="list-style-type: none"> <li>- Điểm CVSS: 8.8 (Cao)</li> <li>- Mô tả: Lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Microsoft Outlook 2016, 2019, Microsoft 365 Apps for Enterprise, Microsoft Office LTSC 2021.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30103">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30103</a>
3	CVE-2024-30078	<ul style="list-style-type: none"> <li>- Điểm CVSS: 8.8 (Cao)</li> <li>- Mô tả: Lỗ hổng trong Windows Wi-Fi Driver cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30078">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30078</a>

4	CVE-2024-30101 CVE-2024-30102 CVE-2024-30104	<ul style="list-style-type: none"> <li>- Điểm CVSS: 7.8 (Cao)</li> <li>- Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Microsoft Outlook 2016, 2019, Microsoft 365 Apps for Enterprise, Microsoft Office LTSC 2021.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30101">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30101</a> <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30102">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30102</a> <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30104">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30104</a>
5	CVE-2024-30100	<ul style="list-style-type: none"> <li>- Điểm CVSS: 7.8 (Cao)</li> <li>- Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, Microsoft SharePoint Server Subscription Edition.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30100">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30100</a>

## 2. Hướng dẫn khắc phục

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. Quý đơn vị tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại link nguồn tham khảo tại mục 1 của Phụ lục.

## 3. Tài liệu tham khảo

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

<https://www.zerodayinitiative.com/blog/2024/6/11/the-june-2024-security-update-review>