

UBND TỈNH TÂY NINH  
**SỞ THÔNG TIN VÀ TRUYỀN THÔNG**

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

Số: /STTTT-TTGSĐH  
V/v cảnh báo lỗ hổng bảo mật có mức ảnh hưởng cao trong các sản phẩm Microsoft công bố tháng 12/2023

Tây Ninh, ngày tháng 01 năm 2024

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các cơ quan tham mưu, giúp việc Tỉnh ủy;
- Mặt trận Tổ quốc và các Đoàn thể chính trị - xã hội;
- Các Sở, ban, ngành tỉnh;
- Các huyện, thị, thành ủy trực thuộc Tỉnh ủy;
- UBND các huyện, thị xã, thành phố;
- UBND các xã, phường, thị trấn;
- Các đơn vị ngành dọc trên địa bàn tỉnh.

Sở Thông tin và Truyền thông nhận Công văn số 2074/CATTT-NCSC của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 12/2023 (***Thông tin chi tiết phụ lục kèm theo***).

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin cho người dùng, đơn vị và toàn bộ hệ thống của tỉnh, Sở Thông tin và Truyền thông đề nghị các đơn vị, địa phương thực hiện gấp các công việc cụ thể như sau:

1. Kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows và phần mềm có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá kịp thời theo hướng dẫn tại phụ lục để tránh nguy cơ bị tấn công.

2. Tăng cường kiểm tra, giám sát hệ thống mạng của đơn vị, địa phương, khi có phát hiện hoạt động tấn công mạng, đề nghị liên hệ Sở Thông tin và Truyền thông để phối hợp xử lý kịp thời.

Thông tin liên quan đề nghị liên hệ Ông Vương Duy Thanh - Trung tâm Giám sát, điều hành kinh tế, xã hội tập trung; Điện thoại: 0932624462./.

Trân trọng!

***Nơi nhận:***

- Như trên;
- BGD Sở (b/c);
- P.CNTTB CVT;
- Lưu: VT, TTGSĐH.

**KT. GIÁM ĐỐC**  
**PHÓ GIÁM ĐỐC**

**PHỤ LỤC**  
**Thông tin các lỗ hổng nghiêm trọng trong các sản phẩm**  
**Microsoft công bố tháng 12/2023**

**1. Thông tin lỗ hổng bảo mật**

**- Mô tả:**

- Lỗ hổng an toàn thông tin **CVE-2023-36019** trong Microsoft Power Platform Connector cho phép đối tượng tấn công thực hiện tấn công giả mạo, dẫn tới thực thi mã từ xa ở phía người dùng.

- 02 lỗ hổng an toàn thông tin **CVE-2023-35630, CVE-2023-35641** trong Internet Connection Sharing (ICS) cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2023-35628** trong Windows MSHTML Platform cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2023-35636** trong Microsoft Outlook làm lộ loạt NTML hash, cho phép đối tượng tấn công thực hiện leo thang đặc quyền.

**- Ảnh hưởng:**

| <b>STT</b> | <b>CVE</b>     | <b>Mô tả</b>  | <b>Link tham khảo</b>  |
|------------|----------------|---|--|
| 1          | CVE-2023-36019 | <p>- Điểm: CVSS: 9.6 (Nghiêm trọng)</p> <p>- Mô tả: Lỗ hổng trong Microsoft Power Platform Connector cho phép đối tượng tấn công thực hiện tấn công giả mạo, dẫn tới thực thi mã từ xa ở phía người dùng.</p> <p>- Ảnh hưởng: Microsoft Power Platform, Azure Logic Apps.</p> | <p><a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE2023-36019">https://msrc.microsoft.com/update-guide/vulnerability/CVE2023-36019</a></p> |

|   |   |   |   |
|---|---|---|---|
| 2 | <p>CVE-2023-35630</p> <p>CVE-2023-35641</p> | <p>- Điểm: CVSS: 8.8 (Nghiêm trọng)</p> <p>- Mô tả: Lỗ hổng trong Internet Connection Sharing (ICS) cho phép đối tượng tấn công thực thi mã từ xa.</p> <p>- Ảnh hưởng: Windows 10, Windows 11; Windows Server 2008, 2012, 2016, 2019, 2022.</p>                                 | <p><a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35630">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35630</a></p> <p><a href="https://msrc.microsoft.com/updateguide/vulnerability/CVE2023-35641">https://msrc.microsoft.com/updateguide/vulnerability/CVE2023-35641</a></p> |
| 3 | <p>CVE-2023-35628</p>                       | <p>Điểm: CVSS: 8.1 (Nghiêm trọng)</p> <p>Mô tả: Lỗ hổng trong Windows MSHTML Platform cho phép đối tượng tấn công thực thi mã từ xa.</p> <p>Ảnh hưởng: Windows 10, Windows 11; Windows Server 2008, 2012, 2016, 2019, 2022.</p>   | <p><a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE2023-35628">https://msrc.microsoft.com/update-guide/vulnerability/CVE2023-35628</a></p>  |
| 4 | <p>CVE-2023-35636</p>                       | <p>- Điểm: CVSS: 6.5 (Cao)</p> <p>- Mô tả: Lỗ hổng trong Microsoft Outlook làm lộ lọt NTML hash, cho phép đối tượng tấn công thực hiện leo thang đặc quyền.</p> <p>- Ảnh hưởng: Microsoft Office 2016, 2019; Microsoft Office LTSC 2021; Microsoft 365 Apps for Enterprise.</p> | <p><a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE2023-35636">https://msrc.microsoft.com/update-guide/vulnerability/CVE2023-35636</a></p>  |

**- Đánh giá mức độ:** Đánh giá sơ bộ từ các chuyên gia bảo mật, lỗ hổng này ảnh hưởng đến nhiều thiết bị trên toàn cầu trong đó có cả Việt Nam. Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) đánh giá khả năng các mã khai thác của các lỗ hổng này sẽ sớm được công khai trên Internet trong thời gian sắp tới.

## **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. Quý đơn vị tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại link nguồn tham khảo.

### **3. Nguồn tham khảo:**

<https://www.zerodayinitiative.com/blog/2023/12/12/the-december-2023-security-update-review>

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