

SỞ THÔNG TIN VÀ TRUYỀN THÔNG CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM  
TỈNH THANH HÓA  
**TRUNG TÂM CNTT&TT**  
**Độc lập - Tự do - Hạnh phúc**

Số: /TTCNTT&TT-QTHT

Thanh Hoá, ngày tháng năm 2023

V/v lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 12/2023.

Kính gửi:

- Văn Phòng Tỉnh ủy;
- Văn Phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn Phòng UBND tỉnh;
- Các sở, ban, ngành cấp tỉnh;
- UBND các huyện, thị xã, thành phố;
- Các tổ chức đoàn thể chính trị cấp tỉnh;
- Các doanh nghiệp VT, CNTT trên địa bàn tỉnh.

Căn cứ Công văn số 2260/CATTT-NCSC ngày 18/12/2023 về việc lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 12/2023 của Cục An toàn thông tin Bộ Thông tin và Truyền thông. Theo đó ngày 12/12/2023, Microsoft đã phát hành danh sách bản vá tháng 12 với 33 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-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.

*(Thông tin chi tiết các lỗ hổng bảo mật có tại Phụ lục kèm theo.)*

Đề tăng cường chủ động phòng ngừa các rủi ro mất an toàn thông tin tại các hệ thống thông tin của các cơ quan, đơn vị, Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa đề nghị các cơ quan, đơn vị chỉ đạo các bộ phận, cá nhân thực hiện những nội dung sau:

1. Kiểm tra, rà soát, xác định máy sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng bởi các lỗ hổng bảo mật được công bố trên. Thực hiện cập nhật bản vá bảo mật đối với các lỗ hổng này kịp thời để tránh nguy cơ bị tấn công. Hướng dẫn kỹ thuật cách thức thực hiện chi tiết đối với lỗ hổng bảo mật tại địa chỉ: <https://attt.thanhhoa.gov.vn>

2. Chỉ đạo các Tổ ứng cứu sự cố an toàn thông tin mạng tại cơ quan, đơn vị mình tăng cường giám sát hoạt động các hệ thống thông tin và sẵn sàng phương án xử lý sự cố 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.

Trong quá trình thực hiện, nếu gặp khó khăn, vướng mắc về kỹ thuật liên quan đến các nội dung, công việc trên đề nghị liên hệ với Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa (*cơ quan thường trực của Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh*) để phối hợp hỗ trợ, xử lý.

Điện thoại: (0237)3718.699

Thư điện tử: [ungcuusuco@thanhhoa.gov.vn](mailto:ungcuusuco@thanhhoa.gov.vn)

Xin trân trọng cảm ơn./.

**Nơi nhận:**

- Như kính gửi;
- Sở TT&TT (để b/c);
- PGĐ Sở Nguyễn Văn Tước (để b/c);
- Giám đốc Trung tâm (để b/c);
- Lưu: VT, QTHT.

**KT. GIÁM ĐỐC  
PHÓ GIÁM ĐỐC**

**Trần Ngọc Hưng**

**Phụ lục:** Thông tin các lỗ hổng bảo mật  
(Kèm theo công văn số /TTCNTT&TT-QTHT ngày tháng năm 2023  
của Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa)

**1. Thông tin các lỗ hổng bảo mật**

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-36019	<ul style="list-style-type: none"> <li>- Điểm: CVSS: 9.6 (Nghiêm trọng)</li> <li>- 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.</li> <li>- Ảnh hưởng: Microsoft Power Platform, Azure Logic Apps.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36019">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36019</a>
2	CVE-2023-35630 CVE-2023-35641	<ul style="list-style-type: none"> <li>- Điểm: CVSS: 8.8 (Nghiêm trọng)</li> <li>- Mô tả: Lỗ hổng trong Internet Connection Sharing (ICS) 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-2023-35630">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35630</a>  <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35641">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35641</a>
3	CVE-2023-35628	<ul style="list-style-type: none"> <li>- Điểm: CVSS: 8.1 (Nghiêm trọng)</li> <li>- Mô tả: Lỗ hổng trong Windows MSHTML Platform cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Windows 10, Windows 11; Windows</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35628">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35628</a>

STT	CVE	Mô tả	Link tham khảo
		Server 2008, 2012, 2016, 2019, 2022.	
4	CVE-2023-35636	<ul style="list-style-type: none"> <li>- Điểm: CVSS: 6.5 (Cao)</li> <li>- Mô tả: Lỗi hỏng trong Microsoft Outlook làm lộ lọt NTML hash, cho phép đối tượng tấn công thực hiện leo thang đặc quyền.</li> <li>- Ảnh hưởng: Microsoft Office 2016, 2019; Microsoft Office LTSC 2021; Microsoft 365 Apps for Enterprise.</li> </ul>	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35636">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35636</a>

## 2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hỏng an toàn thông tin nói trên theo hướng dẫn của hãng. Hướng dẫn chi tiết khắc phục các lỗ hỏng bảo mật trên tại địa chỉ: <https://attt.thanhhoa.gov.vn> (Mục Hướng dẫn → Kỹ năng An toàn thông tin). Các 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.

The screenshot shows the website interface for 'CHUYÊN TRANG AN TOÀN THÔNG TIN TỈNH THANH HÓA'. The navigation bar includes links for 'Trang chủ', 'Tin tức', 'Cảnh báo', 'Hướng dẫn', 'Liên hệ', and 'Báo cáo sự cố'. The 'Hướng dẫn' link is highlighted with a red box, and a dropdown menu is open, showing options: 'Kỹ năng an toàn thông tin', 'Công cụ', 'Bản tin số ATTT', and 'Trắc nghiệm ATTT'. The 'Kỹ năng an toàn thông tin' option is also highlighted with a red box. Below the navigation bar, there are several news items under the heading 'Tin hoạt động':

- Tổ chức lớp bồi dưỡng, tập huấn bảo đảm an toàn thông tin mạng**: Sáng ngày 23/11/2023, tại Tòa nhà Trung tâm Công nghệ thông tin tỉnh, Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa tổ chức khai mạc lớp bồi dưỡng, tập huấn bảo đảm an toàn thông tin mạng.
- Patch Tuesday tháng 11 của Microsoft và 5 lỗ hỏng zero-day mới**: Hình ảnh minh họa với logo Microsoft và một băng dán trên lịch tháng 11.
- Diễn tập thực chiến bảo đảm an toàn thông tin mạng năm 2023**: Hình ảnh minh họa về diễn tập thực chiến.
- Hướng dẫn khắc phục lỗ hỏng bảo mật mới mức độ cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 10/2023**: Hình ảnh minh họa về hướng dẫn khắc phục lỗ hỏng bảo mật.
- Cẩn trọng lộ, lọt thông tin cá nhân trên những ứng dụng mới**: Hình ảnh minh họa về cảnh báo lộ, lọt thông tin cá nhân.

## 3. Tài liệu tham khảo

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

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