UBND TỈNH TUYÊN QUANG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 1787 /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 12/2023

Tuyên Quang, ngày 21 tháng 12 năm 2023

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;
- Uỷ ban nhân dân các huyện, thành phố.

Căn cứ văn bản số 2260/CATTT–NCSC ngày 18/12/2023 của Cục An toàn thông tin về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoftcông bố tháng 12/2023, 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:

1. Thông tin về lỗ hổng bảo mật trong các sản phẩm Microsoft

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 lọt NTML hash, cho phép đối tượng tấn công thực hiện leo thang đặc quyền.

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 cho 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.

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

CỘNG HOÀ X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH TUYÊN QUANG

Nguyễn Văn Hiến

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG AN TOÀN THÔNG TIN TRONG SẢN PHẨM MICROSOFT
(Kèm theo Công văn số 1787 /STTTT-CNTT&BCVT ngày 21 /12/2023 của Sở Thông tin và Truyền thông)

1. Thông tin các lỗ hổng an toàn thông tin

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-36019	- Điểm: CVSS: 9.6 (Nghiêm trọng) - 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. - Ảnh hưởng: Microsoft Power Platform, Azure Logic Apps.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36019
2	CVE-2023-35630 CVE-2023-35641	- Điểm: CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Internet Connection Sharing (ICS) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35630 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35641
3	CVE-2023-35628	- Điểm: CVSS: 8.1 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows MSHTML Platform cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35628

STT	CVE	Mô tả	Link tham khảo
		- Ảnh hưởng: Windows 10, Windows 11; Windows Server 2008, 2012, 2016, 2019, 2022.	
4	CVE-2023-35636	- Điểm: CVSS: 6.5 (Cao) - Mô tả: Lỗ hổng trong Microsoft Outlook làm lộ lọt NTML hash, cho phép đối tượng tấn công thực hiện leo thang đặc quyền. - Ảnh hưởng: Microsoft Office 2016, 2019; Microsoft Office LTSC 2021; Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35636

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/2023/12/12/the-december-2023-security-update-review