UBND TỈNH KIÊN GIANG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số : 2741 /STTTT-CĐS
V/v lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 12/2023

Kiên Giang, ngày 20 *tháng* 12 *năm 2023*

Kính gửi:
- Văn phòng Tỉnh ủy;
- Văn phòng UBND tỉnh;
- Sở, ban, ngành cấp tỉnh;
- UBND các huyện, thành phố;
- Phòng Văn hóa - Thông tin các huyện, thành phố.

Sở Thông tin và Truyền thông Kiên Giang nhận được Công văn số 2260/CATTT-NCSC ngày 18/12/2023 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 12/2023.

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 Microsoft. Bản phát hành tháng 12 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 bảo mật có tại phụ lục kèm theo).

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan, đơn vị trên địa bàn tỉnh, góp phần bảo đảm an toàn cho không gian mạng Việt Nam. Sở Thông tin và Truyền thông Kiên Giang khuyến nghị các cơ quan, đơn vị thực hiện một số biện pháp sau:

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 sau:

- Cục An toàn thông tin - Bộ Thông tin và Truyền thông: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ncsc@ais.gov.vn.

- Hoặc Phòng Chuyển đổi số - Sở Thông tin và Truyền thông Kiên Giang, điện thoại: 0297.3921678, 0918767498 (đ/c Nghỉ), thư điện tử: ttnghi.stttt@kiengiang.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Trung tâm CNTTTT (thực hiện);
- Lưu: VT, CĐS, ttnghi.

GIÁM ĐỐC

CỘNG HÒA XHCN VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH KIÊN GIANG

Võ Minh Trung

PHỤ LỤC
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT
TRONG SẢN PHẨM CỦA MICROSOFT

(Kèm theo Công văn số /STTTT-CĐS ngày / 12 /2023 của Sở Thông tin và Truyền Thông)

1. Thông tin các lỗ hổng an toàn thông tin

STT	CVE	Mô tả	Link cập nhật 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. - Ảnh hưởng: Windows 10, Windows 11;	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35628

STT	CVE	Mô tả	Link cập nhật tham khảo
		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. Các cơ quan, đơn vị tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại "**Link cập nhật tham khảo**" mục 1 của bảng Phụ lục này.

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