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 : 1125 /STTTT-CĐS
V/v lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 05/2024

Kiên Giang, ngày 21 tháng 5 năm 2024

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 884/CATTT-NCSC ngày 16/5/2024 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 05/2024.

Theo đó ngày 14/5/2024, Microsoft đã phát hành danh sách bản vá tháng 05 với **59** lỗ hổng an toàn thông tin trong các sản phẩm của Microsoft. Bản phát hành tháng 05 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-2024-30040** trong Windows MSHTML Platform cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2024-30044** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

- **03** lỗ hổng an toàn thông tin **CVE-2024-30051, CVE-2024-30032, CVE-2024-30035** trong Windows DWM Core Library cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2024-30042** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-30033** trong Windows Search Service cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền.

- Lỗ hổng an toàn thông tin **CVE-2024-30043** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện tấn công XXE.

(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 liên hệ đầu mối hỗ trợ:

- 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.

- Phòng Chuyển đổi số - Sở Thông tin và Truyền thông Kiên Giang, điện thoại: 0918767498 (gặp đ/c Trần Thiện 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 1125 /STTTT-CĐS ngày 21 / 5 /2024
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-2024-30040	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Windows MSHTML Platform cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30040
2	CVE-2024-30044	- Điểm: CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30044
3	CVE-2024-30051 CVE-2024-30032 CVE-2024-30035	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Windows DWM Core Library cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11,	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30051 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30032 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30035

		Windows Server 2016, 2019, 2022.	
4	CVE-2024-30042	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Excel, Office Online Server, Microsoft 365 Apps, Microsoft Office LTSC.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30042
5	CVE-2024-30033	- Điểm: CVSS: 7.0 (Cao) - Mô tả: Lỗ hổng trong Windows Search Service cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30033
6	CVE-2024-30043	- Điểm: CVSS: 6.5 (Cao) - Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện tấn công XXE. - Ảnh hưởng: Microsoft SharePoint Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30043

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 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/2024/5/14/the-may-2024-security-update-review