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 :1666 /STTTT-CĐS
V/v lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 07/2024

Kiên Giang, ngày 16 tháng 7 năm 2024

Kính gửi:
- Sở, ban, ngành cấp tỉnh (Đảng, chính quyền, đoàn thể);
- Ủy ban nhân dân các huyện, thành phố.

Sở Thông tin và Truyền thông Kiên Giang nhận được Công văn số 1310/CATTT-NCSC ngày 12/7/2024 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 07/2024.

Theo đó ngày 09/7/2024, Microsoft đã phát hành danh sách bản vá tháng 07 với **139** lỗ hổng an toàn thông tin trong các sản phẩm của Microsoft. Bản phát hành tháng 07 đặc biệt đáng chú ý vào các lỗ hổng an toàn thông tin có mức ảnh hưởng cao và nghiêm trọng sau:

- 03 lỗ hổng an toàn thông tin **CVE-2024-38074, CVE-2024-38076, CVE-2024-38077** trong Windows Remote Desktop Licensing Service cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng an toàn thông tin **CVE-2024-38060** trong Windows Imaging Component cho phép đối tượng tấn công thực thi mã từ xa.
- 03 lỗ hổng an toàn thông tin **CVE-2024-38023, CVE-2024-38024, CVE-2024-38094** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng an toàn thông tin **CVE-2024-38021** trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.
- Lỗ hổng an toàn thông tin **CVE-2024-38080** trong Windows Hyper-V cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.
- Lỗ hổng an toàn thông tin **CVE-2024-38112** trong Windows MSHTML Platform cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). Lỗ hổng hiện đang bị khai thác trong thực tế.

(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, thư điện tử: ttnghi.stttt@kiengiang.gov.vn.

Trân trọng./.

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

GIÁM ĐỐC

CỘNG HÒA X.H.C.N 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 / 7 /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-2024-38074** **CVE-2024-38076** **CVE-2024-38077**	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Remote Desktop Licensing Service cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38074 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38076 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38077
2	**CVE-2024-38060**	- Điểm CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Imaging Component 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-2024-38060
3	**CVE-2024-38023** **CVE-2024-38024** **CVE-2024-38094**	- Điểm CVSS: 7.2 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38023 https://msrc.microsoft.com/update-

		- Ảnh hưởng: Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, Microsoft SharePoint Server Subscription Edition.	guide/vulnerability/CVE-2024-38024 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38094
4	**CVE-2024-38021**	- Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office 2016, 2019, Microsoft Office LTSC 2021, Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38021
5	**CVE-2024-38080**	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 11, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38080
6	**CVE-2024-38112**	- Điểm CVSS: 7.5 (Cao) - Mô tả: Lỗ hổng trong Windows MSHTML Platform cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38112

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 mục 1 "***Link cập nhật tham khảo***" của bảng Phụ lục này.

3. Tài liệu tham khảo

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

https://www.zerodayinitiative.com/blog/2024/7/9/the-july-2024-security-update-review