UBND TỈNH KIÊN GIANG **SỞ Y TẾ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:1256 /SYT-VP	*Kiên Giang, ngày 30 tháng 4 năm 2024*

V/v cảnh báo lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 04/2024

Kính gửi:
- Các phòng chức năng Sở Y tế;
- Các cơ quan, đơn vị thuộc và trực thuộc Sở Y tế.

(sau đây gọi là đơn vị).

Thực hiện Công văn số 888/STTTT-CĐS ngày 23/4/2024 của Sở Thông tin và Truyền thông tỉnh về việc lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 04/2024; Nâng cao và duy trì hiệu quả đảm bảo an toàn thông tin trong quá trình sử dụng máy tính tại các đơn vị trực thuộc ngành Y tế,

Sở Y tế đề nghị lãnh đạo các đơn vị quan tâm, chú trọng triển khai thực hiện một số nội dung sau:

1. Đơn vị tiến hành kiểm tra, rà soát máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng bởi các lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 04/2024 *(đính kèm phụ lục hướng dẫn)*.

Theo đó ngày 09/4/2024, Microsoft đã phát hành danh sách bản vá tháng 04 với 147 lỗ hổng an toàn thông tin trong các sản phẩm của Microsoft. Bản phát hành tháng 04 đặc biệt đáng chú ý vào các lỗ hổng an toàn thông tin có mức ảnh hưởng cao và nghiêm trọng.

2. Trên cơ sở công tác thực hiện nay tại đơn vị cần quan tâm, tăng cường hơn nữa công tác giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng (nếu chưa phù hợp); 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 triển khai, thực hiện có khó khăn, vướng mắc xin liên hệ Sở Y tế (qua Văn phòng Sở gặp ông Vũ Mạnh Thắng, số điện thoại 0988.202.102) để được trao đổi, hướng dẫn.

Nhận được Công văn này đề nghị lãnh đạo cơ quan, đơn vị quan tâm, thực hiện./.

Nơi nhận:
- Như trên;
- GĐ và các PGĐ Sở Y tế (để b/cáo);
- Trang TTĐT Sở Y tế;
- Trang VPĐT;
- Lưu: VT, vmthang.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ Y TẾ
TỈNH KIÊN GIANG

Nguyễn Trúc Giang

UBND TỈNH KIÊN GIANG
SỞ Y TẾ

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

PHỤ LỤC
Cảnh báo lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 04/2024

(Đính kèm theo Công văn số 1256/SYT-VP ngày 30 /4/2024 của Sở Y tế)

I. Các lỗ hổng an toàn thông tin có mức ảnh hưởng cao và nghiêm trọng:

- Lỗ hổng an toàn thông tin **CVE-2024-20678** trong Remote Procedure Call Runtime (RPC) cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-29988** trong SmartScreen cho phép đối tượng tấn công vượt qua cơ chế bảo vệ.

- **03** lỗ hổng an toàn thông tin **CVE-2024-21322, CVE-2024-21323, CVE-2024-29053** trong Microsoft Defender for IoT cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-20670** trong Outlook for Windows làm lộ lọt NTML hash, cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing).

- Lỗ hổng an toàn thông tin **CVE-2024-26256** trong thư viện nguồn mở libarchive cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-26257** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

- **07** lỗ hổng an toàn thông tin **CVE-2024-26221, CVE-2024-26222, CVE-2024-26223, CVE-2024-26224, CVE-2024-26227, CVE-2024-26231, CVE-2024-26233** trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-26234** trong Proxy Driver cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing).

II. Thông tin các lỗ hổng bảo mật:

STT	Danh sách các lỗi bảo mật máy tính công khai (Common Vulnerabilities and Exposures (**CVE**))	Mô tả	Link cập nhật tham khảo
1	CVE-2024-20678	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Remote Procedure Call Runtime (RPC) 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-2024-20678
2	CVE-2024-29988	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong SmartScreen cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29988
3	CVE-2024-21322 CVE-2024-21323 CVE-2024-29053	- Điểm: CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft Defender for IoT cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Defender for IoT.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21322 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21323 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29053
4	CVE-2024-20670	- Điểm: CVSS: 8.1 (Cao) - Mô tả: Lỗ hổng trong Outlook for Windows làm lộ lọt NTML hash,	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20670

STT	Danh sách các lỗi bảo mật máy tính công khai (Common Vulnerabilities and Exposures (**CVE**))	**Mô tả**	**Link cập nhật tham khảo**
		cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). - Ảnh hưởng: Outlook for Windows.	
5	CVE-2024-26256	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong thư viện nguồn mở libarchive cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 11; Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26256

III. 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 II của Phụ lục này.

IV. Tài liệu tham khảo:

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

- https://www.zerodayinitiative.com/blog/2024/4/9/the-april-2024-security-updates-review