UBND TỈNH KIÊN GIANG
SỞ Y TẾ

Số: 898 /SYT-VP

V/v cảnh báo lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 03/2024

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

Kiên Giang, ngày 26 tháng 3 năm 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 582/STTTT-CĐS ngày 20/3/2024 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 03/2024; Tiếp tục 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 03/2024 *(đính kèm phụ lục hướng dẫn)*. Theo đó, Microsoft vừa phát hành danh sách bản vá lỗi tháng 03/2024 với 59 lỗ hổng an toàn thông tin trong các sản phẩm của Microsoft.

2. Trên cơ sở công tác thực hiện nay tại đơn vị cần 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

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 03/2024

(Đính kèm theo Công văn số 898 /SYT-VP ngày 26/3/2024 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-2024-26198** trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-21407** trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-21408** trong Windows Hyper-V cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ (DoS).

- Lỗ hổng an toàn thông tin **CVE-2024-21334** trong Open Management Infrastructure (OMI) cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-21426** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-21411** trong Skype for Consumer cho phép đối tượng tấn công thực thi mã từ xa.

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 tham khảo
01	CVE-2024-26198	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng:	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26198

STT	Danh sách các lỗi bảo mật máy tính công khai (Common Vulnerabilities and Exposures (**CVE**))	**Mô tả**	**Link tham khảo**
		Microsoft Exchange Server 2016, 2019.	
02	CVE-2024-21407	- Điểm: CVSS: 8.1 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2012, 2012 R2, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE- 2024-21407
03	CVE-2024-21408	- Điểm: CVSS: 5.5 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ (DoS). - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE- 2024-21408
04	CVE-2024-21334	- Điểm: CVSS: 9.8 (Cao) - Mô tả: Lỗ hổng trong Open Management Infrastructure (OMI) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: OMI; System Center Operations Manager	https://msrc.microsoft.com/update-guide/vulnerability/CVE- 2024-21334

STT	Danh sách các lỗi bảo mật máy tính công khai (Common Vulnerabilities and Exposures (**CVE**))	**Mô tả**	**Link tham khảo**
		(SCOM) 2019, 2022.	
	CVE-2024-21426	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Enterprise Server 2016, Microsoft SharePoint Server 2019; Microsoft SharePoint Server Subscription Edition.	https://msrc.microsoft.com/update-guide/vulnerability/CVE- 2024-21426
	CVE-2024-21411	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Skype for Consumer cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Skype for Consumer.	https://msrc.microsoft.com/update-guide/vulnerability/CVE- 2024-21411

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 tham khảo**" mục II của Phụ lục này.

IV. Tài liệu tham khảo:

- https://msrc.microsoft.com/update-guide/
- https://www.zerodayinitiative.com/blog/2024/3/12/the-march-2024-security-update-review