UBND HUYỆN CÁT TIÊN **PHÒNG VĂN HÓA VÀ THÔNG TIN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 42 /VHTT	*Cát Tiên, ngày 25 tháng 3 năm 2024*

V/v cảnh báo lỗ hổng bảo mật trong các sản phẩm Microsoft công bố tháng 03/2024 và tháo gỡ mã độc

Kính gửi:
- Các cơ quan, đơn vị trên địa bàn huyện;
- UBND các xã, thị trấn.

Căn cứ Văn bản số 301/STTTT-TTTHDL&CĐS ngày 22/03/2024 của Sở Thông tin và Truyền thông về việc lỗ hổng bảo mật trong các sản phẩm Microsoft công bố tháng 03/2024 và cảnh báo đơn vị có IP nằm trong mạng Botnet tháng 03/2024.

Ngày 12/3/2024, Microsoft đã phát hành danh sách bản vá tháng 03 với 59 lỗ hổng an toàn thông tin trong các sản phẩm của mình. Bản phát hành tháng này 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-2024-26198** 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. *(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 nhà nước trên địa bàn huyện, Phòng Văn hóa và Thông tin đề nghị các cơ quan, đơn vị, UBND các xã, thị trấn triển khai một số nội dung, cụ thể như sau:

1. Tiếp tục kiểm tra, rà soát, xác định các máy tính sử dụng hệ điều hành Windows, Office 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. Chỉ đạo cán bộ, công chức, viên chức tiếp tục cài đặt các phần mềm diệt vi rút (đảm bảo 100% máy tính có phần mềm diệt vi rút). Thường xuyên quét vi rút trên các máy tính để tháo gỡ mã độc tồn tại trong mạng nội bộ của đơn vị (mỗi máy tính thực hiện quét vi rút tối thiểu 01 lần/ ngày).

4. Thường xuyên thực hiện việc sao lưu dữ liệu định kỳ cho hệ thống máy chủ và máy trạm tại đơn vị.

5. Phối hợp với chuyên môn của Phòng Văn hóa và Thông tin trong việc kiểm tra, rà soát và xử lý mã độc khi có yêu cầu.

* Trong trường hợp cần hỗ trợ, xin vui lòng liên hệ:

- Ông Nguyễn Xuân Tùng - Trưởng phòng CNTT - Sở TTTT. Điện thoại: 02633.541.542 hoặc 0975.886.197.

- Ông Phan Minh Hoàng - Trung tâm tích hợp dữ liệu và Chuyển đổi số - Sở TTTT. Điện thoại: 0984.497.451.

- Ông Vũ Văn Tự - Chuyên viên Phòng Văn hóa và Thông tin. Điện thoại 02633.884.092 hoặc 0865. 254.585.

Trên đây là cảnh báo lỗ hổng bảo mật trong các sản phẩm Microsoft công bố tháng 3/2024 và tháo gỡ mã độc. Kính đề nghị các cơ quan, đơn vị quan tâm triển khai thực hiện đảm bảo an toàn, an ninh thông tin./.

Nơi nhận:
- Như kính gửi;
- UBND huyện (b/c);
- Trang TTĐT huyện;
- Lưu: VT, VHTT.

TRƯỞNG PHÒNG

PHÒNG VĂN HÓA VÀ THÔNG TIN

Lê Ngọc Dũng

PHỤ LỤC

Thông tin về các lỗ hổng bảo mật trong sản phẩm Microsoft tháng 3/2024

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	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: Microsoft Exchange Server 2016, 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26198
2	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
3	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;	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21408

		Windows Server 2016, 2019, 2022.	
4	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 (SCOM) 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21334
5	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
6	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

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng bảo mật 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 nguồn tham khảo tại mục 1 của phụ lục.

3. Tài liệu tham khảo

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

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