ỦY BAN NHÂN DÂN **HUYỆN GIA LÂM**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 864 /UBND-VHTT V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 3/2024	*Gia Lâm, ngày 26 tháng 3 năm 2024*

Kính gửi:
- Các cơ quan chuyên môn, đơn vị, trường học thuộc Huyện;
- UBND các xã, thị trấn.

Thực hiện Công văn số 684/STTTT-ATTT&GDĐT ngày 20/3/2024 của Sở Thông tin và Truyền thông Hà Nội về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 3/2024;

Nhằm đảm bảo an toàn thông tin cho hệ thống, góp phần bảo đảm an toàn không gian mạng, UBND huyện đề nghị các cơ quan chuyên môn, đơn vị, UBND xã, thị trấn, trường học trên địa bàn huyện thực hiện một số nội dung sau:

1. Kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng bởi các lỗ hổng bảo mật như CVE-2024-26198 trong Microsoft Exchange Sever, CVE-2024-21426 trong Microsoft SharePoint Sever,…Thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công. Thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công.

2. Chủ động, tăng cường giám sát các hệ thống thông tin của cơ quan, sẵn sàng phương án xử lý khi có dấu hiệu khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng, các tổ chức lớn về an toàn thông tin để phát hiện kịp thời nguy cơ tấn công mạng và các lỗ hổng bảo mật.

3. Trong quá trình tổ chức thực hiện, nếu có khó khăn vướng mắc đề nghị các đơn vị liên hệ Đội ứng cứu sự cố an toàn thông tin mạng Thành phố Hà Nội (điện thại trực 24/24: 024.35124010; Email: ttdt_sotttt@hanoi.gov.vn).

Đề nghị các cơ quan, đơn vị quan tâm, thực hiện./.

Nơi nhận: - Như trên; - Lưu: VT, VHTT.	**TM. ỦY BAN NHÂN DÂN** **KT. CHỦ TỊCH** **PHÓ CHỦ TỊCH** **Trương Văn Học**

Phụ lục

THÔNG TIN VỀ CÁC LỖ HỔNG AN TOÀN THÔNG TIN TRONG SẢN PHẨM MICROSOFT

(Kèm theo Công văn số /UBND-VHTT ngày /3/2024 của UBND huyện)

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-26198	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Exchange Sever cho phép đối tượng tấn công thực thi mã từ xa - Ảnh hưởng: Microsoft Exchange Sever 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, 11; Windows Sever 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; Windows Sever 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21408
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 Sever cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Enterprise Sever 2019, Microsoft SharePoint Sever 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

*** 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 đơn vị tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại link nguồn tham khảo tại Phụ lục.

*** Tài liệu tham khảo**

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

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