ỦY BAN NHÂN DÂN **HUYỆN BÌNH CHÁNH**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 1523 /UBND	*Bình Chánh, ngày 25 tháng 4 năm 2024*
V/v cập nhật bản vá các lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft	

Kính gửi: Thủ trưởng các đơn vị:
- Cơ quan chuyên môn và đơn vị sự nghiệp (kể cả sự nghiệp giáo dục);
- Ủy ban nhân dân xã, thị trấn.

Căn cứ Công văn số 940/STTTT-CNTT ngày 20 tháng 3 năm 2024 của Sở Thông Tin và Truyền Thông về lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft; thông tin Microsoft đã phát hành danh sách các bản vá lỗ hổng bảo mật trong các sản phẩm của mình. Bản phát hành đặc biệt lưu ý các lỗ hổng bảo mật có mức độ ảnh hưởng cao và nghiêm trọng *(Đính kèm phụ lục)*.

Căn cứ Quyết định số 2236/QĐ-UBND ngày 19 tháng 3 năm 2024 của Ủy ban nhân dân huyện Bình Chánh về ban hành Quy chế phối hợp ứng phó, khắc phục sự cố đảm bảo an toàn, an ninh mạng đối với các hệ thống thông tin của huyện Bình Chánh. Ủy ban nhân huyện Bình Chánh có ý kiến chỉ đạo như sau:

1. Đề nghị Thủ trưởng các cơ quan, đơn vị và Chủ tịch Ủy ban nhân dân xã, thị trấn

- Tăng cường quán triệt và tuyên truyền đến cán bộ, công chức, viên chức và người lao động về Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của các cơ quan, đơn vị quản lý nhà nước huyện Bình Chánh ban hành kèm theo Quyết định số 6469/QĐ-UBND ngày 17 tháng 8 năm 2022 của Ủy ban nhân dân huyện Bình Chánh và Quy chế phối hợp ứng phó, khắc phục sự cố đảm bảo an toàn, an ninh mạng đối với các hệ thống thông tin của huyện Bình Chánh ban hành kèm theo Quyết định số 2236/QĐ-UBND ngày 19 tháng 3 năm 2024 của Ủy ban nhân dân huyện Bình Chánh; nâng cao ý thức trách nhiệm trong việc sử dụng hệ thống thông tin, thực hiện tốt các biện pháp bảo đảm an toàn, an ninh mạng; nhằm chủ động phòng ngừa lộ thông tin nội bộ, bí mật nhà nước qua mạng Internet.

- Căn cứ vào tình hình thực tế, phân công cán bộ, công chức và viên chức có năng lực, kỹ năng về tin học triển khai, tự thực hiện hoặc xem xét thuê dịch

vụ phù hợp với nhu cầu của đơn vị; 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 nhằm giảm thiểu nguy cơ bị tấn công, kể cả cá nhân sử dụng các sản phẩm Microsoft trong công việc.

- Tăng cường các biện pháp bảo mật cơ bản: thường xuyên cập nhật phần mềm diệt virus và phần mềm bảo mật khác; Hạn chế truy cập vào các trang web không an toàn và các email lạ; Tăng cường kiểm soát truy cập vào hệ thống thông tin nội bộ của đơn vị.

- Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bất kỳ dấu hiệu khai thác, tấn công mạng; báo cáo ngay cho Trung tâm dữ liệu và ứng dụng công nghệ thông tin Huyện *(Thông qua đầu mối: Ông Nguyễn Hoàng Tuân, thành viên Trung tâm, số điện thoại di động 0909.545.797 và email: nhtuan.binhchanh@tphcm.gov.vn)* để được hướng dẫn ứng phó, khắc phục sự cố, đối với các hệ thống thông tin dùng chung của huyện Bình Chánh.

2. Giao Trung tâm Dữ liệu và Ứng dụng Công nghệ thông tin Huyện

- Tăng cường giám sát và chủ động các phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng.

- Thường xuyên tổ chức kiểm tra, đánh giá thực trạng an toàn thông tin tại huyện Bình Chánh, tập trung giám sát, theo dõi quy trình quản lý văn bản số, email, quy trình cập nhật thông tin và các quy định bảo mật hiện tại của hệ thống thông tin của huyện Bình Chánh; nghiên cứu, đề xuất Ủy ban nhân dân Huyện ban hành quy định về quản lý, sử dụng, sửa chữa, thanh lý các thiết bị kỹ thuật điện tử thông tin, viễn thông phục vụ công tác bảo vệ bí mật nhà nước.

- Tham mưu tăng cường áp dụng các giải pháp đảm bảo an toàn an ninh thông tin; thường xuyên khảo sát, đánh giá, kiểm tra chi tiết, toàn bộ hệ thống mạng, nâng cao chất lượng hệ thống cảnh báo, giám sát tự động cho mạng nội bộ và chủ động thực hiện công tác giám sát, cảnh báo từ xa đối với hệ thống thông tin điện tử, không để đối tượng xấu có điều kiện xâm nhập, phá hoại./.

Nơi nhận:
- Như trên;
- TTUB;
- CVP, PCVP;
- Lưu: VP-Tin học.

CHỦ TỊCH

Võ Đức Thanh

PHỤ LỤC

Thông tin về các lỗ hổng bảo mật trong sản phẩm của Microsoft

(Kèm theo Công văn số 1523 /UBND ngày 25 tháng 4 năm 2024 của Ủy ban nhân dân huyện Bình Chánh)

1. Thông tin các lỗ hổng an toàn thông tin

a	CVE	Mô tả	Link tham khảo
1.	CVE-2024-20674	Điểm: CVSS: 9.0 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Kerberos cho phép đối tượng tấn công vượt qua cơ chế bảo vệ để thực hiện tấn công giả mạo. - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20674
2.	CVE-2024-21318	Điểm: CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server 2016, 2019; Microsoft SharePoint Server Subscription Edition.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21318
3.	CVE-2024-20677	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20677

a	CVE	Mô tả	Link tham khảo
		mã từ xa. - Ảnh hưởng: Microsoft Office 2019; Microsoft Office LTSC; Microsoft 365 Apps.	
4.	CVE-2024-20700	- Điểm: CVSS: 7.5 (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 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20700
5.	CVE-2024-21410	- Điểm: CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ trong Microsoft Exchange Server cho phép đối tượng không cần xác thực thực hiện tấn công leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft Exchange Server 2016, 2019	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21410
6.	CVE-2024-21413 CVE-2024-21378	- Điểm: CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công không	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21413 https://msrc.microsoft.co

a	CVE	Mô tả	Link tham khảo
		cần xác thực thực thi mã từ xa. - Ảnh hưởng: Microsoft Office, Microsoft Office LTSC, Microsoft 365 Apps for Enterprise, Microsoft Outlook.	m/update-guide/vulnerability/CVE-2024-21378
7.	CVE-2024-21399	- Điểm: CVSS: 8.3 (Trung bình) - Mô tả: Lỗ hổng trong Microsoft Edge (Chromium-based) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Edge (Chromium-based).	https://msrc.microsoft.com/update-guide/vulnerability/CVE2024-21399
8.	CVE-2024-21412	- Điểm: CVSS: 8.1 (Cao) - Mô tả: Lỗ hổng trong Internet Shortcut Files cho phép đối tượng tấn công vượt qua cơ chế bảo mật. Lỗ hổng hiện đan bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE2024-21412
9.	CVE-2024-21379	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Word cho phép đối tượng tấn công thực thi	https://msrc.microsoft.com/update-guide/vulnerability/CVE2024-21379

a	CVE	Mô tả	Link tham khảo
		mã từ xa. - Ảnh hưởng: Microsoft Word, Microsoft Office, Microsoft Office LTSC, Microsoft 365 Apps for Enterprise	
10.	CVE-2024-21384	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office OneNote cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office LTSC, Microsoft 365 Apps for Enterprise	https://msrc.microsoft.com/update-guide/vulnerability/CVE2024-21384
11.	CVE-2024-20673	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office LTSC, Microsoft Office, Skype for Business.	https://msrc.microsoft.com/update-guide/vulnerability/CVE2024-20673
12.	CVE-2024-21351	- Điểm: CVSS: 7.6 (Cao) - Mô tả: Lỗ hổng trong Windows SmartScreen cho phép đối tượng tấn công vượt qua cơ chế bảo mật. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10,	https://msrc.microsoft.com/update-guide/vulnerability/CVE2024-21351

a	CVE	Mô tả	Link tham khảo
		Windows 11, Windows Server 2016, 2019, 2022	

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 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/2024/1/9/the-january-2024-security-update-review

https://www.zerodayinitiative.com/blog/2024/2/13/the-february-2024-security-update-review