SAO Y; ỦY BAN NHÂN DÂN QUẬN 12; Thời gian ký: 2025-02-19T14:34:55+07:00

ỦY BAN NHÂN DÂN QUẬN 12	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1070 /UBND-VHTT V/v lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft	*Quận 12, ngày 19 tháng 02 năm 2025*

Kính gửi:
- Các cơ quan tham mưu giúp việc Quận ủy;
- Ủy ban MTTQ Việt Nam quận;
- Ban chỉ huy Công an quận;
- Các phòng, ban ngành, trung tâm, công ty thuộc quận;
- Bệnh viện quận;
- Ủy ban nhân dân 11 phường.

Ủy ban nhân dân quận nhận được Công văn số 369/STTTT-CNTT ngày 05 tháng 02 năm 2025 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 công bố tháng 12/2024. Theo đó, Microsoft đã phát hành danh sách bản vá tháng 12 với 72 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 *(Đính kèm phụ lục)*.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin tại các đơn vị, Ủy ban nhân dân quận đề nghị các đơn vị:

1. 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 để tránh nguy cơ bị tấn công.

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. Đầu mối hỗ trợ: Đội ứng cứu sự cố an toàn thông tin mạng Thành phố

- Số điện thoại hotline 24/7: 0889490111.
- Số điện thoại trong giờ hành chính: 38233717 ext: 111.
- Thư điện tử: ATTT@tphcm.gov.vn.

Ủy ban nhân dân quận đề nghị các đơn vị nghiêm túc thực hiện./.

Nơi nhận:
- Như trên;
- UBND quận (CT);
- VP.UBND quận;
- Phòng VHTT;
- Lưu: VT, Tg.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Nguyễn Minh Chánh

PHỤ LỤC

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

(Đính kèm Công văn số ..1070../UBND-VHTT ngày 19.. tháng 02.. năm 2025 của UBND Quận 12)

1. Thông tin các lỗ hổng an toàn thông tin

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-49138	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Windows Common Log File System Driver cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022, 2025.	https://msrc.microsoft.com/updateguide/vulnerability/CVE2024-49138
2	CVE-2024-49112 CVE-2024-49127	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Lightweight Directory Access Protocol (LDAP) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022, 2025.	https://msrc.microsoft.com/updateguide/vulnerability/CVE2024-49112 https://msrc.microsoft.com/updateguide/vulnerability/CVE2024-49127
3	CVE-2024-49117	- Điểm CVSS: 8.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa.	https://msrc.microsoft.com/updateguide/vulnerability/CVE2024-49117

STT	CVE	Mô tả	Link tham khảo
		- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2022, 2025.	
4	CVE-2024-49124	- Điểm CVSS: 8.1 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Lightweight Directory Access Protocol (LDAP) Client cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022, 2025.	https://msrc.microsoft.com/updateguide/vulnerability/CVE2024-49124
5	CVE-2024-49126	- Điểm CVSS: 8.1 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows Local Security Authority Subsystem Service (LSASS) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022, 2025.	https://msrc.microsoft.com/updateguide/vulnerability/CVE2024-49126
6	CVE-2024-49070	- Điểm CVSS: 7.4 (Cao) - Mô tả: Lỗ hổng trong Microsoft SharePoint cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019, Microsoft	https://msrc.microsoft.com/updateguide/vulnerability/CVE2024-49070

STT	CVE	Mô tả	Link tham khảo
		SharePoint Enterprise Server 2016.	
7	CVE-2024-49068	- Điểm CVSS: 8.2 (Cao) - Mô tả: Lỗ hổng trong Microsoft SharePoint cho phép đối tượng tấn công thực hiện leo thang đặc quyền. - Ảnh hưởng: Microsoft SharePoint Server Subscription Edition, Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016.	https://msrc.microsoft.com/updateguide/vulnerability/CVE2024-49068
8	CVE-2024-49142	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Access cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Access 2016, Microsoft Office LTSC 2021, 2024, Microsoft 365 Apps for Enterprise, Microsoft Office 2019.	https://msrc.microsoft.com/updateguide/vulnerability/CVE2024-49142
9	CVE-2024-9069	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Excel 2016, Microsoft Office LTSC 2021, 2024, Microsoft 365 Apps for Enterprise, Microsoft Office 2019.	https://msrc.microsoft.com/updateguide/vulnerability/CVE2024-49069

STT	CVE	Mô tả	Link tham khảo
10	CVE-2024-49065	- Điểm CVSS: 5.5 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Word 2016, Microsoft Office LTSC 2021, 2024, Microsoft 365 Apps for Enterprise, Microsoft Office 2019, Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016.	https://msrc.microsoft.com/updateguide/vulnerability/CVE2024-49065

2. Hướng dẫn khắc phục

Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng.

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.

Kiểm tra, rà soát, xác định máy tính sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. 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.

3. Tài liệu kham khảo

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

https://www.zerodayinitiative.com/blog/2024/12/10/the-december-2024-security-update-review