UBND THÀNH PHỐ BẮC KẠN
PHÒNG VĂN HÓA VÀ THÔNG TIN

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

Số:92 /VHTT

TP. Bắc Kạn, ngày 27 tháng 5 năm 2024

V/v thông báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 5/2024

Kính gửi:
- Ủy ban MTTQ và các đoàn thể thành phố;
- Các phòng, ban, đơn vị thành phố;
- Ủy ban nhân dân xã, phường.

Thực hiện Công văn số 617/STTTT-CNTT-BCVT ngày 21/5/2024 của Sở Thông tin và Truyền thông tỉnh Bắc Kạn về việc thông báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 5/2024. Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các phòng, ban, ngành, đoàn thể, Uỷ ban nhân dân xã, phường, Phòng Văn hoá và Thông tin thành phố Bắc Kạn thông báo các lỗ hổng bảo mật để các đơn vị biết, triển khai thực hiện các giải pháp về an toàn thông tin với nội dung như sau:

1. Các lỗ hổng bảo mật

- Lỗ hổng an toàn thông tin **CVE-2024-30040** trong Windows MSHTML Platform cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2024-30044** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

- **03** lỗ hổng an toàn thông tin **CVE-2024-30051, CVE-2024-30032, CVE-2024-30035** trong Windows DWM Core Library cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế.

- Lỗ hổng an toàn thông tin **CVE-2024-30042** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2024-30033** trong Windows Search Service cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền.

- Lỗ hổng an toàn thông tin **CVE-2024-30043** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện tấn công XXE.

(Thông tin chi tiết các lỗ hổng bảo mật theo phụ lục gửi kèm).

3. Đề nghị các cơ quan, đơn vị thực hiện một số biện pháp đảm bảo an toàn thông tin như sau:

- Kiểm tra, rà soát các phần mềm PAN-OS đang sử dụng có khả năng bị ảnh hưởng bởi lỗ hổng trên. Thực hiện nâng cấp lên phiên bản mới nhất để tránh nguy cơ bị tấn công (*Tham khảo thông tin tại phụ lục gửi kèm theo*)

- Kiểm tra, rà soát, xác định máy 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 *(tham khảo thông tin tại phụ lục kèm theo).*

- 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.

Trong quá trình thực hiện nếu phát hiện hoặc khó khăn, vướng mắc về thông tin lỗ hổng bảo mật đề nghị các cơ quan, đơn vị liên hệ Phòng Văn hóa và Thông tin thành phố Bắc Kạn *(bà Lâm Thị Trang, điện thoại 0969155599)* hoặc Sở thông tin và Truyền thông *(phòng Công nghệ thông tin, điện thoại: 0209 3871 626)* để phối hợp giải quyết.

Với nội dung trên đề nghị các cơ quan, đơn vị triển khai thực hiện./.

Nơi nhận:
Gửi bản điện tử:
- Như trên;
- CT, PCT UBND TP (Ô. Trưởng);
- Lưu: VHTT.

KT. TRƯỞNG PHÒNG
PHÓ TRƯỞNG PHÒNG PHỤ TRÁCH

CỘNG HÒA X.H.C.N VIỆT NAM
PHÒNG VĂN HÓA VÀ THÔNG TIN
TP. BẮC KẠN T. BẮC KẠN

Lường Văn Thiết

Phụ lục

THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT TRONG SẢN PHẨM MICROSOFT

(Kèm theo Công văn số /VHTT ngày /5/2024 của Phòng văn hoá và Thông tin thành phố Bắc Kạn)

1. Thông tin các lỗ hổng an toàn thông tin

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-30040	- Điểm: CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Windows MSHTML Platform cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30040
2	CVE-2024-30044	- 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.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30044
3	CVE-2024-30051 CVE-2024-30032 CVE-2024-30035	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Windows DWM Core Library cho phép đối tượng	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30051 https://msrc.microsoft.com/update-guide/vulnerability/CVE-

		tấn công thực hiện tấn công leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2016, 2019, 2022.	2024-30032 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30035
4	CVE-2024-30042	- 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, Office Online Server, Microsoft 365 Apps, Microsoft Office LTSC.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30042
5	CVE-2024-30033	- Điểm: CVSS: 7.0 (Cao) - Mô tả: Lỗ hổng trong Windows Search Service cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30033

6	CVE-2024-30043	- Điểm: CVSS: 6.5 (Cao) - Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện tấn công XXE. - Ảnh hưởng: Microsoft SharePoint Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30043

2. 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 mục 1 của Phụ lục.

3. Tài liệu tham khảo

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

https://www.zerodayinitiative.com/blog/2024/5/14/the-may-2024-security-update-review