UỶ BAN NHÂN DÂN **THÀNH PHỐ BẮC NINH**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 113/UBND-VHTT V/v cảnh báo, phát hiện, xử lý đảm bảo an toàn thông tin, lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2023	*Thành phố Bắc Ninh, ngày 16 tháng 01 năm 2023*

Kính gửi:
- Các phòng, ban, đơn vị thuộc UBND thành phố;
- UBND các phường.

Thực hiện Công văn số 33/STTTT-CNTT ngày 13/01/2023 của Sở Thông tin và Truyền thông tỉnh Bắc Ninh về việc lỗ hổng bảo mật ảnh hưởng mức Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2023;

Tại Công văn số 50/CATTT-NCSC ngày 11/01/2023 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về lỗ hổng bảo mật ảnh hưởng mức Cao và Nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2022 trong đó đã phát hành danh sách bản vá tháng 01 với 98 lỗ hổng bảo mật trong các sản phẩm của mình. Bản phát hành tháng này đặc biệt đáng chú ý các lỗ hổng bảo mật có mức ảnh hưởng cao và nghiêm trọng, cụ thể như sau:

- Lỗ hổng bảo mật **CVE-2023-21674** trong Windows Advanced Local Procedure Call (ALPC) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế.

- 03 lỗ hổng bảo mật **CVE-2023-21743, CVE-2023-21744, CVE-2023-21742** trong Microsoft SharePoint Server, trong đó **CVE-2023-21743** cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật; 02 lỗ hổng **CVE-2023-21744, CVE-2023-21742** cho phép đối tượng tấn công thực thi mã từ xa.

- 04 lỗ hổng bảo mật **CVE-2023-21763, CVE-2023-21764, CVE-2023-21762, CVE-2023-21745** trong Microsoft Exchange Server, trong đó 02 lỗ hổng **CVE 2023-21763, CVE-2023-21764** cho phép đối tượng tấn công thực hiện nâng cao đặc quyền; 02 lỗ hổng **CVE-2023-21762, CVE-2023-21745** cho phép đối tượng tấn công thực hiện tấn công giả mạo.

- Lỗ hổng bảo mật **CVE-2023-21549** trong Windows Workstation Service cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã được công bố rộng rãi trên Internet.

- 02 lỗ hổng bảo mật **CVE-2023-21561, CVE-2023-21551** trong Microsoft Cryptographic Services cho phép đối tượng tấn công nâng cao đặc quyền.

- 02 lỗ hổng bảo mật **CVE-2023-21734, CVE-2023-21735** trong Microsoft Office 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).

Để đảm bảo kịp thời xử lý, khắc phục các lỗ hổng bảo mật về an toàn thông tin cho hệ thống thông tin của các cơ quan, đơn vị và UBND các phường trên địa bàn thành phố Bắc Ninh (nếu có).

UBND thành phố yêu cầu các cơ quan, đơn vị và UBND các phường triển khai thực hiện tốt một số nhiệm vụ sau:

1. 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.

(Thực hiện theo 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 về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

3. Ngay khi phát hiện sự cố, nếu các cơ quan, đơn vị và UBND các phường không có khả năng xử lý yêu cầu thông báo về đầu mối Trung tâm Công nghệ Thông tin và Truyền thông - Sở Thông tin và Truyền thông tỉnh Bắc Ninh để được hỗ trợ xử lý, khắc phục kịp thời.

*** Đầu mối liên hệ:**

1. Đồng chí: Lại Hữu Dương - Phó Giám đốc Trung tâm CNTT&TT, Sở Thông tin và Truyền thông tỉnh, số điện thoại 0913.629.199.

2. Đồng chí: Nguyễn Thế Thủy - Phòng Quản trị và Tích hợp hệ thống - Trung tâm CNTT&TT, Sở Thông tin và Truyền thông tỉnh, số điện thoại 0222.3875606 hoặc 0929003888.

- Địa chỉ thư điện tử: pqtthht.stttt@bacninh.gov.vn.

Yêu cầu các cơ quan, đơn vị và UBND các phường nghiêm túc triển khai thực hiện./.

Nơi nhận:
- Như kính gửi (t/h);
- TT Thành ủy - HĐND thành phố (b/c);
- Chủ tịch, các PCT UBND thành phố;
- Lưu: VT, VHTT.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Nguyễn Mạnh Hiếu

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

(Kèm theo Công văn số 113/UBND-VHTT ngày 16/01/2023 của UBND Thành phố Bắc Ninh)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-21674	- Điểm: CVSS: 8.8 (cao) - Mô tả: lỗ hổng trong Windows Advanced Local Procedure Call (ALPC) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2019/2022.	https://msrc.microsoft. com/update guide/vulnerability/CV E-2023-21674
2	CVE-2023-21743, CVE-2023-21744, CVE-2023-21742	- Điểm: CVSS: 8.8 (cao) - Mô tả: lỗ hổng trong trong Microsoft SharePoint Server cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass), thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2019/2022.	https://msrc.microsoft. com/update guide/vulnerability/CV E-2023-21743 https://msrc.microsoft. com/update guide/vulnerability/CV E-2023-21744 https://msrc.microsoft. com/update guide/vulnerability/CV E-2023-21742
3	CVE-2023-21763, CVE-2023-21764, CVE-2023-21762, CVE-2023-21745	- Điểm: CVSS: 8.0/7.8 (cao) - Mô tả: lỗ hổng trong trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện nâng cao đặc quyền, tấn công giả mạo (Spoofing). - Ảnh hưởng: Microsoft Exchange Server 2016/2019.	https://msrc.microsoft. com/update guide/vulnerability/CV E-2023-21763 https://msrc.microsoft. com/update guide/vulnerability/CV E-2023-21764 https://msrc.microsoft. com/update guide/vulnerability/CV E-2023-21762 https://msrc.microsoft. com/update guide/vulnerability/CV E-2023-21745

4	CVE-2023-21549	- Điểm: CVSS: 8.8 (cao) - Mô tả: lỗ hổng trong Windows Workstation Service cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã được công bố rộng rãi trên Internet. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2012/2019/2022.	https://msrc.microsoft. com/update guide/vulnerability/CV E-2023-21549
5	CVE-2023-21561, CVE-2023-21551	- Điểm: CVSS: 8.8/7.8 (cao) - Mô tả: lỗ hổng trong Microsoft Cryptographic Services cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/ 2022.	https://msrc.microsoft. com/update guide/vulnerability/CV E-2023-21561 https://msrc.microsoft. com/update guide/vulnerability/CV E-2023-21551
6	CVE-2023-21734, CVE-2023-21735	- 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 for Mac 2021, Microsoft 365, Microsoft Office 2019 for Mac.	https://msrc.microsoft. com/update guide/vulnerability/CV E-2023-21734 https://msrc.microsoft. com/update guide/vulnerability/CV E-2023-21735

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. 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/2023/1/10/the-january-2023- security-update-review.