UỶ BAN NHÂN DÂN **HUYỆN BẠCH THÔNG**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 115 /UBND-VHTT V/v Thông báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2023.	*Bạch Thông, ngày tháng 01 năm 2023*

Kính gửi:

- Các cơ quan chuyên môn, đơn vị sự nghiệp thuộc huyện;
- UBND các xã, thị trấn.

Ngày 13/01/2023, UBND huyện nhận được Văn bản số 42/STTTT-CNTT-BCVT của Sở Thông tin và Truyền thông tỉnh về việc thông báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2023. Nhằm bảo đảm an toàn thông tin cho hệ thống thông tin của huyện, Uỷ ban nhân dân huyện thông báo các lỗ hổng bảo mật 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 bảo đảm an toàn thông tin, UBND huyện đề nghị các đơn vị triển khai thực hiện một số nội dung 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 *(tham khảo thông tin tại 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 lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

Trong quá trình thực hiện nếu có khó khăn, vướng mắc đề nghị các đơn vị liên hệ với Sở thông tin và Truyền thông để phối hợp giải quyết (*phòng Công nghệ thông tin-Bưu chính Viễn thông điện thoại: 0209 871626 hoặc ông Nguyễn Văn Cương, điện thoại 0989 332 044 hoặc bà Đinh Thị Xuyên, chuyên viên phòng VHTT huyện, SĐT: 0986 967 906*).

UBND huyện đề nghị các cơ quan, đơn vị quan tâm, triển khai thực hiện./.

Nơi nhận:
Gửi bản điện tử:
- Như trên;
- Thường trực Huyện uỷ;
- Thường trực HĐND huyện;
- Chủ tịch, PCT (VX) UBND huyện;
- VP HĐND - UBND huyện (P/h);
- Lưu: VT.

TM. UỶ BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Nguyễn Duy Luân

Phụ lục

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

(Kèm theo Công văn số /UBND-VHTT, ngày / 01 /2023 của UBND huyện Bạch Thông)

1. Thông tin các lỗ hổng bảo mật

TT	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/CVE-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/CVE-2023-21743 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21744 https://msrc.microsoft.com/update-guide/vulnerability/CVE-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	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21763 https://msrc.microsoft.com/update-guide/vulnerability/CV

		công giả mạo (Spoofing). - Ảnh hưởng: Microsoft Exchange Server 2016/2019.	E-2023-21764 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21762 https://msrc.microsoft.com/update-guide/vulnerability/CVE-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/CVE-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/CVE-2023-21561 https://msrc.microsoft.com/update-guide/vulnerability/CVE-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	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21734 https://msrc.microsoft.com/update-guide/vulnerability/CV

		2021, Microsoft 365, Microsoft Office 2019 for Mac.	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