UBND TỈNH ĐIỆN BIÊN **SỞ Y TẾ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 1822/SYT-VP V/v cảnh báo lỗ hổng bảo mật ảnh hưởng Cao trong các sản phẩm Microsoft công bố tháng 9/2022	*Điện Biên, ngày 07 tháng 10 năm 2022*

Kính gửi: Các đơn vị trực thuộc Sở Y tế.

Căn cứ Công văn số 1578/STTTT-CNTT ngày 27/9/2022 của Sở Thông tin và Truyền thông về lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm Microsoft công bố tháng 9/2022. Để đảm bảo an toàn thông tin cho hệ thống thông tin trong ngành Y tế. Sở Y tế đề nghị các cơ quan, đơn vị trực thuộc thực hiện ngay một số nội dung như 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 theo dõi giám sát hệ thống và có phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng.

3. Phối hợp với Trung tâm CNTT&TT Sở Thông tin và Truyền thông kiểm tra, rà soát, kịp thời xử lý đối với các hệ thống hiện đang quản lý; bố trí bộ phận ứng cứu sự cố hỗ trợ các đơn vị khắc phục sự cố khi có yêu cầu.

Đầu mối hỗ trợ, ứng cứu an ninh mạng Sở Thông tin và Truyền thông: Đ/c Mai Xuân Dũng - Phòng Công nghệ Thông tin, điện thoại: 0914.599.177; Đ/c Nguyễn Mạnh Cường - Trung tâm CNTT&TT, điện thoại 0946.560.568.

Văn phòng Sở Y tế: Đ/c. Phan Quốc Toản - Phó Chánh Văn phòng Sở Y tế, ĐT: 3831777 - 0915350789 Email: toanpq.syt@dienbien.gov.vn.

Nhận được văn bản này Sở Y tế đề nghị Lãnh đạo các cơ quan, đơn vị trực thuộc chỉ đạo triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Các phòng CN;
- GĐ và các PGĐ Sở Y tế;
- Lưu: VT, VP.

GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ Y TẾ
TỈNH ĐIỆN BIÊN

Phạm Giang Nam

PHỤ LỤC
THÔNG TIN VỀ LỖ HỔNG BẢO MẬT
TRONG SẢN PHẨM MICROSOFT
(Kèm theo Công văn số /SYT-VP ngày /10/2022 của Sở Y tế)

1. Thông các tin lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-37969	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Windows Common Log File System Driver cho phép đối tượng tấn công thực thi mã từ xa với các đặc quyền nâng cao. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37969
2	CVE-2022-34718	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows TCP/IP cho phép đối tượng tấn công chưa xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34718
3	CVE-2022-34724	- Điểm CVSS: 7.5 (Cao) - Lỗ hổng trong Windows DNS Server cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ. - Ảnh hưởng: Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34724
4	CVE-2022-3075	- Lỗ hổng trong Chromium cho phép đối tượng tấn công chưa xác thực có thể thực thi mã từ xa. - Ảnh hưởng: Microsoft Egde (Chromium-based)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-3075

5	CVE-2022-34721, CVE-2022-34722	- Điểm CVSS: 9.8 (Nghiêm trọng) - Lỗ hổng trong Windows Internet Key Exchange (IKE) Protocal Extensions cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 7/8.1/10/11, Windows Server 2008/2012/2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34721 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34722
6	CVE-2022-37961 CVE-2022-35823 CVE-2022-38008 CVE-2022-38009	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SherePoint Foundation 2013, SharePoint Server 2013/2016/2019, Microsoft SharePoint Enterprise Server 2013.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37961 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-35823 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38008 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38009
7	CVE-2022-37962	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoít PowerPoint cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office 2013/2016/2019, Office 365 Apps, Office LTSC 2021.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-37962

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. 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. Nguồn tham khảo

https://msrc.microsoft.com/update-guide/releaseNote/2022-Aug

https://www.zerodayinitiative.com/blog/2022/8/9/theaugust-2022-security-update-review