UBND TỈNH ĐIỆN BIÊN **SỞ Y TẾ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 749 /SYT-VP V/v Lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 4/2023.	*Điện Biên, ngày 25 tháng 4 năm 2023*

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

Căn cứ Công văn số 349/CNTT-YTĐT ngày 20/4/2023 của cục Công nghệ Thông tin Bộ Y tế về lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 04/2023. 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 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 *(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 trường hợp cần thiết, đề nghị đơn vị liên hệ với Trung tâm Dữ liệu y tế, Cục Công nghệ thông tin, Bộ Y tế (ThS. Hoàng Đăng Trị, điện thoại: 0987772483; Email: trihd.cntt@moh.gov.vn) để được hỗ trợ.

Văn phòng Sở Y tế: Đồng chí Phạm Ngọc Hiếu - Văn phòng Sở Y tế, ĐT: 3831777 - 0365336275 Email: phamhieuds@gmail.com.

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;
- Lãnh đạo Sở Y tế;
- Các phòng chức năng - SYT;
- Lưu: VT, VP.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

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

Vừ A Sử

PHỤ LỤC
THÔNG TIN VỀ LỖ HỔNG BẢO MẬT
TRONG SẢN PHẨM MICROSOFT
(Kèm theo Công văn số: /SYT-VP ngày /4/2023của Sở Y tế)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-28252	- Điểm: CVSS: 7.8 (cao) - Mô tả: lỗ hổng trong Windows Common Log File System Driver cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Windows Server, Windows 10,11	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2023-28252
2	CVE-2023-21554	- Điểm: CVSS: 9.8 (nghiêm trọng) - Mô tả: lỗ hổng trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2023-21554
3	CVE-2023-23384 CVE-2023-23375 CVE-2023-28304	- Điểm: CVSS: 7.8/7.3 (cao) - Mô tả: lỗ hổng trong Microsoft SQL Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SQL Server, Microsoft ODBC Driver 18.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2023-23384 https://msrc.microsoft.com/updateguide/vulnerability/CVE-2023-23375 https://msrc.microsoft.com/updateguide/vulnerability/CVE-2023-28304
4	CVE-2013-3900	- Điểm: CVSS: 7.4 (cao) - Mô tả: lỗ hổng xác thực chữ ký WinVerifyTrust cho phép đối tượng tấn công có thể thêm nội dung vào phần chữ ký mã xác thực trong tệp thực thi đã ký mà không làm mất hiệu lực chữ ký.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2013-3900

		- Ảnh hưởng: Windows Server, Windows 10/11	
5	CVE-2023-28287 CVE-2023-28295	Điểm: CVSS: 8.8 (cao) - Mô tả: lỗ hổng trong Microsoft Publisher cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office, Microsoft Publisher.	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2023-28287 https://msrc.microsoft.com/updateguide/vulnerability/CVE-2023-28295
6	CVE-2023-28309 CVE-2023-28314	- Điểm: CVSS: 7.6/6.1 (cao) - Mô tả: lỗ hổng trong Microsoft Dynamics 365 cho phép đối tượng tấn công thực hiện tấn công XSS. - Ảnh hưởng: Microsoft Dynamics 365	https://msrc.microsoft.com/updateguide/vulnerability/CVE-2023-28309 https://msrc.microsoft.com/updateguide/vulnerability/CVE-2023-28314

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/2023/4/11/the-april-2023 securityupdate-review