UBND TỈNH ĐIỆN BIÊN
SỞ Y TẾ

Số: 559 /SYT-VP
V/v Lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 03/2023.

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Điện Biên, ngày 29 tháng 3 năm 2023

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

Căn cứ Công văn số 233/CNTT-YTĐT ngày 21/03/2023 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 03/2023. 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, Quý Đơn vị liên hệ 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: Đ/c 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;
- Các phòng chuyên môn SYT;
- Giám Đốc – SYT (Báo cáo);
- Các Đồng chí PGĐ Sở Y tế;
- 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 /3/2023của Sở Y tế)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2023-23397	- Điểm: CVSS: 9.1 (nghiêm trọng) - Mô tả: lỗ hổng trong Microsoft Outlook 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: Microsoft Outlook, Microsoft Office.	https://msrc.microsoft.com/updateguide/vulnerability/CVE2023-23397
2	CVE-2023-24880	- Điểm: CVSS: 5.4 (trung bình) - Mô tả: lỗ hổng trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Lỗ hổng này đang bị khai thác trong thực tế. - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/updateguide/vulnerability/CVE2023-24880
3	CVE-2023-23392	- Điểm: CVSS: 9.8 (nghiêm trọng) - Mô tả: lỗ hổng trong HTTP Protocol Stack cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server, Windows 11.	https://msrc.microsoft.com/updateguide/vulnerability/CVE2023-23392
4	CVE-2023-23415	- Điểm: CVSS: 9.8 (nghiêm trọng) - Mô tả: lỗ hổng trong Internet Control Message Protocol (ICMP) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server, Windows 10/11.	https://msrc.microsoft.com/updateguide/vulnerability/CVE2023-23415

5	CVE-2023-23399	- 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 Office, Microsoft Excel, Microsoft 365 .	https://msrc.microsoft.com/updateguide/vulnerability/CVE2023-23399
6	CVE-2023-23400	- Điểm: CVSS: 7.2 (cao) - Mô tả: lỗ hổng trong Windows DNS Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows Server.	https://msrc.microsoft.com/updateguide/vulnerability/CVE2023-23400

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/2023/3/14/the-march-2023-securityupdate-review