UBND TỈNH ĐIỆN BIÊN **SỞ Y TẾ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 2151 /SYT-VP V/v Cảnh báo lỗ hổng bảo mật ảnh hưởng Cao trong các sản phẩm Microsoft công bố tháng 11/2022	*Điện Biên, ngày 24 tháng 11 năm 2022*

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

Thực hiện Công văn số 1881/STTTT-CNTT ngày 14/11/2022 của Sở Thông tin và Truyền thông về lỗ hổng bảo mật ảnh hưởng cao trong các sản phẩm Microsoft công bố tháng 11/2022. 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 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 /11/2022 của Sở Y tế)

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2022-41082, CVE-2022-41040, CVE-2022-41080, CVE-2022-41079, CVE-2022-41078, CVE-2022-41123	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong Microsoũ Exchange Server cho phép đối tượng tấn công thực thi mã từ xa, nâng cao đặc quyền. - Ảnh hưởng: Microsoft Exchange Server 2016 CU 23/22, Exchange Server 2019 CU 11, Exchange Server 2013 CU 23	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41082 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41040 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41080 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41123 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41078 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41079
2	CVE-2022-41128, CVE-2022-41118	- Điểm CVSS: 8.8 (Cao) - Lỗ hổng trong trong Windows Scripting Languages cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này đang bị khai thác trong thực tế. - Anh hưởng: Windows Server 2008/2012/2016/2019/2022, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41128 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41118

3	CVE-2022-41091	- Điểm CVSS: 5.4 (Trung bình) - Lỗ hổng trong Windows Mark of the Web cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật. Anh hưởng: Windows 10/11, Windows Server 2016/2019/2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41091
4	CVE-2022-41073	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng Windows Print Spooler cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Anh hưởng: Windows Server 2008/2012/2016/2019/2022, Windows 11/10/8.1/7.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41073
5	CVE-2022-41125	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng Windows CNG Key Insolation Service cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. - Anh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019/2022	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41125
6	CVE-2022-41044, CVE-2022-41088, CVE-2022-41039	- Điểm CVSS: 8.1 (Cao) - Lỗ hổng trong Windows Point-to-Point cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 8.1/10/11, Windows Server 2012/2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41044 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41088 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41039

7	CVE-2022-41105, CVE-2022-41106, CVE-2022-41063, CVE-2022-41104	- Điểm CVSS: 7.8 (Cao) - Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa, tấn công giả mạo (Spoofing), thực hiện tấn công vượt qua cơ chế bảo mật. - Ảnh hưởng: Microsoft Excel 2013/2016, Microsoft Office, Microsoft 365.	https://msrc.microsoit.com /update-guide/vulnerability/CVE-2022-41105 https://msrc.microsoft.com /update-guide/vulnerability/CVE-2022-41106 https://msrc.microsoft.com /update-guide/vulnerability/CVE-2022-41063 https://msrc.microsoft.com /update-guide/vulnerability/CVE-2022-41104

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/releaseNote/2022-Nov

https://www.zerodayinitiative.com/blog/2022/11/8/the-november-2022-security-update-review