UBND TỈNH BÀ RỊA-VŨNG TÀU **SỞ Y TẾ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1728/SYT-NV	*Bà Rịa-Vũng Tàu, ngày 30 tháng 05 năm 2023*
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 5/2023.	

Kính gửi: Thủ trưởng các cơ quan, đơn vị trực thuộc.

Sở Y tế nhận được Công văn số 964/STTTT-VTCNT ngày 24/5/2023 của Sở Thông tin và Truyền thông về việc cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 5/2023;

Theo đó, hãng Microsoft đã phát hành danh sách bản vá tháng 05 với 38 lỗ hổng bảo mật trong các sản phẩm của mình, đặc biệt là các lỗ hổng bảo mật ảnh hưởng mức Cao và Nghiêm trọng như sau:

- Lỗ hổng bảo mật **CVE-2023-24955** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. Ngoài ra, 02 lỗ hổng bảo mật được công bố với mã là CVE-2023-21744, CVE-2023-21742 cũng liên quan đến Microsoft SharePoint Server, đã được Sở Thông tin và Truyền thông triển khai tại Công văn số 71/STTTT-VTCNTT ngày 13/01/2023. Điều đó cho thấy, Microsoft SharePoint Server đã và đang là mục tiêu nhắm đến của nhiều đối tượng tấn công mạng nhằm thực hiện các hành động trái phép. Chính vì vậy, các cơ quan, tổ chức cần đặc biệt quan tâm và có phương án khắc phục, xử lý kịp thời nếu bị ảnh hưởng.

- 02 lỗ hổng bảo mật **CVE-2023-29336, CVE-2023-24902** trong Win32k cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế.

- Lỗ hổng bảo mật **CVE-2023-24941** trong Windows Network File System; lỗ hổng bảo mật **CVE-2023-29344** trong Microsoft Office; lỗ hổng bảo mật **CVE-2023-24953** trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng bảo mật **CVE-2023-29325** trong Windows OLE cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng bảo mật **CVE-2023-24932** trong Secure Boot cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass). Các lỗ hổng này đã được công bố rộng rãi trên Internet.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin, Sở Y tế đề nghị các cơ quan, đơn vị đang sử dụng các sản phẩm của Microsoft thực hiện thực hiện kiểm tra, rà soát, xác định các thiết bị có khả năng bị ảnh hưởng, thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công. Thông tin chi tiết các lỗ hổng

bảo mật như trong Công văn số 729/CATTT-NCSC ngày 15/5/2023 của Cục An toàn thông tin kèm theo.

Trong trường hợp cần hỗ trợ xử lý, ứng cứu và khắc phục sự cố, đề nghị liên hệ với các đầu mối hỗ trợ:

- Đầu mối điều phối ứng cứu sự cố quốc gia:

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);

Cục An toàn thông tin; điện thoại: 0869100320; Email: ais@mic.gov.vn.

Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC); điện thoại: 02436404421 hoặc số điện thoại trực đường dây nóng ứng cứu sự cố: 0869100317; Email: ir@vncert.vn.

Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC); điện thoại: 02432091616 hoặc số điện thoại trực đường dây nóng hỗ trợ giám sát, cảnh báo sớm: 0336666905; Email: ais@mic.gov.vn.

- Đầu mối Sở Thông tin và Truyền thông tỉnh Bà Rịa-Vũng Tàu:

Ông Trang Mạch Hoàng Nguyên, Phòng Viễn Thông - Công nghệ thông tin; điện thoại: 0909813717; Email: nguyentmh@ sotttt.baria-vungtau.gov.vn

Ông Phạm Huỳnh Quang Vinh, Trung tâm CNTT và Truyền thông tỉnh; điện thoại: 090 838 0621; Email: vinhphq@sotttt.baria-vungtau.gov.vn

- Đầu mối Sở Y tế: Bà Nguyễn Thị Kim Ngân, Phòng Nghiệp vụ; điện thoại: 0889033054; Email: nganntk@soyte.baria-vungtau.gov.vn

Đề nghị các cơ quan, đơn vị nghiêm túc triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Các Phó Giám đốc SYT;
- Trang TTĐT SYT;
- Lưu: VT, NV.

GIÁM ĐỐC

SỞ Y TẾ

Phạm Minh An