

Số: /SYT-NV

Bà Rịa-Vũng Tàu, ngày tháng năm 2023

V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 7/2023.

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

Sở Y tế nhận được Công văn số 1474/STTTT-CĐSBCVT ngày 20/7/2023 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 7/2023.

Theo đó, hãng Microsoft đã phát hành danh sách bản vá tháng 07 với 130 lỗ hổng bảo mật trong các sản phẩm của mình, đặc biệt các lỗ hổng bảo mật ảnh hưởng mức Cao và Nghiêm trọng như sau:

- 04 lỗ hổng an toàn thông tin **CVE-2023-33160, CVE-2023-33134** trong Microsoft SharePoint Server và **CVE-2023-32057, CVE-2023-35309** trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa.

- Lỗ hổng an toàn thông tin **CVE-2023-36884** trong Office và Windows cho phép đối tượng tấn công thực thi mã từ xa khi người dùng mở tệp tài liệu của Microsoft Office do đối tượng tấn công tạo ra; Lỗ hổng an toàn thông tin **CVE-2023-35311** trong Microsoft Outlook và **CVE-2023-32049** trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật (Bypass); Lỗ hổng an toàn thông tin **CVE-2023-36874** trong Windows Error Reporting Service và **CVE-2023-32046** trong Windows MSHTML cho phép đối tượng tấn công thực hiện tấn công nâng cao đặc quyền. Các lỗ hổng này đang bị khai thác trong thực tế.

Ngoài ra, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin đã cảnh báo rộng rãi về những lỗ hổng ảnh hưởng đến Microsoft SharePoint Server, đề nghị các cơ quan, đơn vị trực thuộc rà soát lỗ hổng liên quan đến Microsoft SharePoint Server để phát hiện và có phương án xử lý kịp thời; tăng cường giám sát nhằm giảm thiểu nguy cơ bị tấn công thông qua các lỗ hổng này.

Đồng thời, Sở Y tế đề nghị các cơ quan, đơn vị đang sử dụng các sản phẩm của Microsoft 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 1261/CATTT-NCSC ngày 17/7/2023 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 Trí; 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;
- Giám đốc SYT (b/cáo);
- Các Phó Giám đốc SYT;
- Trang TTĐT SYT;
- Lưu: VT, NV.

**KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Bùi Chí Tình