

Số: /SYT-NV

Bà Rịa-Vũng Tàu, ngày tháng 01 năm 2023

V/v cảnh báo lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 01/2023.

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

Sở Y tế nhận được Công văn số 71/STTTT-VTCNTT ngày 13/01/2023 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 01/2023.

Theo đó, hãng Microsoft đã phát hành danh sách bản vá tháng 01 với 98 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:

- Lỗ hổng bảo mật **CVE-2023-21674** trong Windows Advanced Local Procedure Call (ALPC) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đang bị khai thác trong thực tế.

- 03 lỗ hổng bảo mật **CVE-2023-21743, CVE-2023-21744, CVE-2023-21742** trong Microsoft SharePoint Server, trong đó **CVE-2023-21743** cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật; 02 lỗ hổng **CVE-2023-21744, CVE-2023-21742** cho phép đối tượng tấn công thực thi mã từ xa.

- 04 lỗ hổng bảo mật **CVE-2023-21763, CVE-2023-21764, CVE-2023-21762, CVE-2023-21745** trong Microsoft Exchange Server, trong đó 02 lỗ hổng **CVE-2023-21763, CVE-2023-21764** cho phép đối tượng tấn công thực hiện nâng cao đặc quyền; 02 lỗ hổng **CVE-2023-21762, CVE-2023-21745** cho phép đối tượng tấn công thực hiện tấn công giả mạo.

- Lỗ hổng bảo mật **CVE-2023-21549** trong Windows Workstation Service cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã được công bố rộng rãi trên Internet.

- 02 lỗ hổng bảo mật **CVE-2023-21561, CVE-2023-21551** trong Microsoft Cryptographic Services cho phép đối tượng tấn công nâng cao đặc quyền.

- 02 lỗ hổng bảo mật **CVE-2023-21734, CVE-2023-21735** trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa.

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 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 50/CATTT-NCSC ngày 11/01/2023 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 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);

- 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: 0254.3512226, 0909813717; thư điện tử: nguyentmh@sotttt.bariavungtau.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 tỉnh Bà Rịa-Vũng Tàu: Bà Nguyễn Thị Kim Ngân, Phòng Nghiệp vụ; điện thoại 0889033054; thư điện tử: nganntk@soyte.bariavungtau.gov.vn.

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

Nơi nhận :

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

GIÁM ĐỐC

Phạm Minh An