

UBND TỈNH BÀ RỊA-VŨNG TÀU
SỞ Y TẾ

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

Số: /SYT-NV

Bà Rịa-Vũng Tàu, ngày tháng 12 năm 2022

V/v cảnh báo lỗ hổng bảo mật ảnh hưởng Cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 10/2022.

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

Sở Y tế nhận được Công văn số 2340/STTTT-VTCNTT ngày 25/12/2022 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 10/2022;

Theo đó, ngày 13/12/2022, Microsoft đã phát hành danh sách bản vá tháng 12 với 52 lỗ hổng bảo mật trong các sản phẩm của mình, trong đó có các lỗ hổng bảo mật ảnh hưởng mức Cao và Nghiêm trọng như sau:

- Lỗ hổng bảo mật **CVE-2022-44698** trong Windows SmartScreen cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật. Lỗ hổng này đang bị khai thác trong thực tế.

- Lỗ hổng bảo mật **CVE-2022-41076** trong PowerShell cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng này ảnh hưởng đến nhiều sản phẩm như: Microsoft Exchange Server, Skype for Business Server,...

- Lỗ hổng bảo mật **CVE-2022-44713** trong Microsoft Outlook for Mac cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing).

- Lỗ hổng bảo mật **CVE-2022-44699** trong Azure Network Watcher Agent cho phép đối tượng tấn công thực hiện tấn công vượt qua cơ chế bảo mật.

- Lỗ hổng **CVE-2022-44710** trong DirectX Graphics Kernel cho phép đối tượng tấn công thực hiện nâng cao đặc quyền. Lỗ hổng này đã có mã khai thác được công bố rộng rãi trên Internet.

- 02 lỗ hổng bảo mật **CVE-2022-44690, CVE-2022-44693** trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa.

- 02 lỗ hổng bảo mật **CVE-2022-44678, CVE-2022-44681** trong Windows Print Spooler cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

- 02 lỗ hổng bảo mật **CVE-2022-44708, CVE-2022-41115** trong Microsoft Edge (Chromium-based) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

- Lỗ hổng bảo mật **CVE-2022-44673** trong Windows Client Server Run-Time Subsystem (CSRSS) cho phép đối tượng tấn công thực hiện nâng cao đặc quyền.

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 được nêu trong Công văn số 2035/CATTT-NCSC 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

