

Số: 4073/SYT-VP

Bình Thuận, ngày 02 tháng 12 năm 2020

V/v cảnh báo nguy cơ tấn công  
vào các cơ quan, tổ chức trong lỗ  
hổng WebLogic

Kính gửi: Các cơ quan, đơn vị trực thuộc

Thực hiện Công văn số 827/CNTT-YTDT ngày 01/12/2020 của Cục công nghệ thông tin - Bộ Y tế về việc cảnh báo nguy cơ tấn công vào các cơ quan tổ chức trong lỗ hổng WebLogic;

Theo đó, ngày ngày 29/10/2020, Cục An toàn thông tin - Bộ Thông tin và Truyền thông có ban hành Công văn số 974/CATTT-NCSC thông về việc cảnh báo nguy cơ tấn công vào các cơ quan tổ chức trong lỗ hổng WebLogic, cụ thể như sau:

- Trong thời gian gần đây Oracle đã công bố nhiều lỗ hổng, trong đó có lỗ hổng CVE-2020-14882 (nghiêm trọng) trên các máy chủ web sử dụng ứng dụng Oracle Weblogic, lỗ hổng này cho phép đối tượng tấn công vượt qua cơ chế xác thực để thực thi các đoạn mã lệnh nguy hiểm và chiếm quyền quản trị hệ thống.

- Hiện tại, một số nhóm chuyên thực hiện tấn công APT có dấu hiệu tận dụng lỗ hổng này để tấn công sâu vào hệ thống thông tin của các cơ quan tổ chức.

Nhằm đảm bảo an toàn thông tin cho các hệ thống thông tin ngành y tế, Sở Y tế đề nghị các cơ quan, đơn vị trực thuộc thực hiện một số nội dung, cụ thể như sau:

- Kiểm tra, rà soát các máy chủ web có sử dụng Oracle Weblogic để phát hiện và xử lý kịp thời nguy cơ tấn công thông qua lỗ hổng này. Trong trường hợp đã có dấu hiệu tấn công cần thực hiện rà soát toàn bộ máy chủ và hệ thống liên quan để phát hiện và loại bỏ các tập tin độc hại, mã độc mà đối tượng tấn công để lại trên hệ thống.

- Cập nhật bản vá lỗ hổng bảo mật cho ứng dụng. Trong trường hợp chưa thể cập nhật bản vá cần triển khai các biện pháp để hạn chế, ngăn chặn việc khai thác lỗ hổng.

- Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ như sau:

+ Trung tâm dữ liệu y tế, Cục Công nghệ thông tin, Bộ Y tế.

+ Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại: 02432091616, thư điện tử: [ais@mic.gov.vn](mailto:ais@mic.gov.vn).

+ Trung tâm Công nghệ thông tin và Truyền thông (đơn vị thường trực Đội ứng cứu sự cố mạng máy tính tỉnh), đường Phạm Hùng, Tp. Phan Thiết, Bình Thuận. SĐT:0252.3750.293.

Đề nghị các cơ quan, đơn vị triển khai thực hiện các nội dung trên./.

***Nơi nhận:***

- Như trên;
- Sở Thông tin và Truyền thông;
- Lưu: VT, VP.

**GIÁM ĐỐC**

**Nguyễn Quốc Việt**