UBND TỈNH ĐỒNG NAI
SỞ Y TẾ

Số: 1305 /SYT-VP

V/v triển khai Công văn số 116/CNTT-DLYT ngày 10/3/2020 của Cục CNTT Bộ Y tế

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

Đồng Nai, ngày 19 tháng 3 năm 2020

Kính gửi: Giám đốc, Thủ trưởng các đơn vị trực thuộc.

Thực hiện Công văn số 116/CNTT-DLYT ngày 10/3/2020 của Cục Công nghệ thông tin Bộ Y tế về việc cảnh báo nguy cơ tấn công vào các máy chủ web sử dụng Apche (*Đính kèm Công văn*).

Giám đốc Sở Y tế đề nghị Giám đốc, Thủ trưởng các đơn vị trực thuộc chỉ đạo các tổ chức, cá nhân phụ trách về công nghệ thông tin của đơn vị tổ chức triển khai thực hiện nội dung Công văn số 116/CNTT-DLYT ngày 10/3/2020 của Cục Công nghệ thông tin Bộ Y tế.

Đề nghị Giám đốc, Thủ trưởng các đơn vị trực thuộc triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Lưu: VT, VP.

GIÁM ĐỐC

Phan Huy Anh Vũ

Số 2 - Phan Đình Phùng, phường Quang Vinh, thành phố Biên Hoà, tỉnh Đồng Nai
ĐT: (02513) 942641, Fax: (02513) 847269, Email: syt@dongnai.gov.vn, Website: syt.dongnai.gov.vn

BỘ Y TẾ
CỤC CÔNG NGHỆ THÔNG TIN

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

Số: 116 /CNTT-DLYT
V/v cảnh báo nguy cơ tấn công vào các máy chủ web sử dụng Apache

Hà Nội, ngày 10 tháng 03 năm 2020

Kính gửi:
- Các Vụ/Cục, Tổng Cục, Văn phòng Bộ, Thanh tra Bộ;
- Các đơn vị trực thuộc Bộ Y tế;
- Sở Y tế các tỉnh, thành phố trực thuộc Trung ương.

(Sau đây gọi tắt là các đơn vị)

Căn cứ Công văn số 135/CATTT-NCSC ngày 9/3/2020 của Cục An toàn thông tin về việc nguy cơ tấn công vào các máy chủ web sử dụng Apache Tomcat thông qua lỗ hổng CVE-2020-1938 (còn gọi là Ghostcat) trong thành phần Apache JServ Protocol của các máy chủ web sử dụng Apache Tomcat (phiên bản 9/8/7 và các phiên bản cũ hơn).

Lỗ hổng bảo mật này đã có mã khai thác công khai trên Internet và thông qua khai thác lỗ hổng đối tượng tấn công có thể thu thập thông tin nội dung các tệp trên máy chủ Tomcat bao gồm cả tập tin cấu hình. Ngoài ra, nếu ứng dụng web cho phép người dùng tải tệp lên, thì đối tượng tấn công có thể lợi dụng để tải lên máy chủ các đoạn mã khai thác và thực thi nhiều hành động độc hại khác.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của quý đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Cục Công nghệ thông tin đề nghị quý đơn vị thực hiện:

1. Rà soát các máy chủ Apache Tomcat để phát hiện và xử lý kịp thời các máy chủ có khả năng đã bị đối tượng tấn công khai thác thông qua lỗ hổng trên. Danh sách phiên bản Tomcat bị ảnh hưởng *tại Phụ lục 1*.

2. Vá lỗ hổng **CVE-2020-1938**, theo cách sau vô hiệu hoá thành phần lỗi hoặc nâng cấp lên phiên bản Apache Tomcat mới. Các phiên bản Apache Tomcat đã được khắc phục lỗi cho từng phiên bản đã có trên https://tomcat.apache.org.

3. Thực hiện theo dõi giám sát và đánh giá an toàn thông tin định kỳ cho các hệ thống thông tin để kịp thời phát hiện và xử lý các nguy cơ gây mất an toàn thông tin.

Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục Công nghệ thông tin: KS. Nguyễn Viết Hưng – Trung tâm Dữ liệu y tế; email: hungnv.cntt@moh.gov.vn; điện thoại: 098 353 9556.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Nguyễn Thanh Long (để b/c);
- Phó Cục trưởng (để biết);
- Lưu: VT, DLYT.

CỤC TRƯỞNG

Trần Quý Tường

BỘ Y TẾ
CỤC CÔNG NGHỆ THÔNG TIN

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

PHỤ LỤC
Danh sách phiên bản Tomcat bị ảnh hưởng

(Kèm theo Công văn số 116/CNTT-DLYT ngày 10/3/2020)

Phiên bản lỗi	Phiên bản đã khắc phục lỗi
Apache Tomcat 9 (9.x < 9.0.31)	9.0.31
Apache Tomcat 8 (8.x < 8.5.51)	8.5.51
Apache Tomcat 7 (7.x < 7.0.100)	7.0.100