PHIẾU GIẢI QUYẾT VĂN BẢN ĐẾN

SỞ Y TẾ
TỈNH KHÁNH HÒA

Số đến:.....
Ngày đến:.....
Lưu hồ sơ:.....

Nơi ban hành: .....
Số và ký hiệu văn bản: .....
Ngày ban hành: ..... Thời hạn xử lý: .....
Đơn vị chủ trì: ..... Đơn vị phối hợp: .....

*Ý kiến của lãnh đạo cơ quan: .....
Chuyển VP triển khai
.....
.....
.....
.....

Ngày 10 tháng 7 năm 2015

*Ý kiến của Trưởng/Phó đơn vị:.....
.....
.....
.....
.....

*Ý kiến đề xuất của người giải quyết:.....
.....
.....
.....

*Tiến độ giải quyết:

Ngày chuyển VB:..... Ngày trình VB trả lời: .....
Ngày ban hành VB trả lời:..... Số, ký hiệu VB trả lời: .....
Đánh giá thời gian hoàn thành: Trước hạn ☐ Đúng hạn ☐ Trễ hạn ☐

BỘ Y TẾ
CỤC CÔNG NGHỆ THÔNG TIN

Số: 220 /CNTT-CSHT
V/v rà soát, tăng cường đảm bảo an toàn thông tin trên môi trường mạng

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

Hà Nội, ngày 10 tháng 7 năm 2015

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

Hiện nay, việc đảm bảo an toàn thông tin thông tin là yêu cầu hết sức quan trọng, đặc biệt là các thông tin được lưu trữ, truyền đưa trên môi trường mạng. Nhằm hạn chế các sự cố mất an toàn thông tin và tăng cường bảo vệ an ninh, an toàn hệ thống mạng thông tin quốc gia, Cục Công nghệ thông tin kính đề nghị các đơn vị thực hiện các hoạt động sau:

1. Tiến hành kiểm tra, rà quét toàn bộ hệ thống nhằm phát hiện và khắc phục các lỗ hổng bảo mật, đặc biệt là các lỗ hổng phổ biến như:

- Lỗ hổng *Blind SQL Injection*. Đây là lỗ hổng bảo mật rất nghiêm trọng của lập trình viên khi xây dựng, phát triển trang thông tin điện tử do không kiểm tra chặt chẽ dữ liệu đầu vào cho phép tin tặc thực thi câu lệnh truy vấn bất hợp pháp chiếm quyền quản trị trang thông tin điện tử. Đáng chú ý, tin tặc có thể lợi dụng lỗ hổng này để khai thác tài khoản quản trị hệ thống thông tin, chiếm quyền điều khiển server. Cụ thể, đã thu thập được toàn bộ thông tin về tài khoản quản trị trên trang *mch.moh.gov.vn* bao gồm tên đăng nhập, mật khẩu mã hóa, số điện thoại, địa chỉ email, thời gian đăng nhập...

- Lỗ hổng *Cross site scripting (XSS)*. Lợi dụng lỗ hổng bảo mật này tin tặc có thể tấn công đánh cắp thông tin người dùng, thực thi một số truy cập bất hợp pháp tới máy chủ web. Khai thác lỗi bảo mật trên, tin tặc có thể chèn các đoạn mã độc hại lên máy chủ web hoặc kết hợp sử dụng hình thức tấn công Social Engineering để đánh cắp phiên truy cập của người dùng (session cookie).

- Lỗ hổng *Slow HTTP Denial of Service Attack*. Lợi dụng lỗ hổng bảo mật này tin tặc sẽ gửi gói tin liên tục làm treo hệ thống (vì hệ thống sẽ xử lý gói tin một cách tuần tự).

- Lỗ hổng *Host Header Attach*. Lợi dụng lỗ hổng bảo mật này tin tặc sẽ chèn các đoạn mã độc hại vào Host header (thông qua việc gửi các gói tin request), máy chủ sẽ thực thi các lệnh mà tin tặc mong muốn.

2. Có biện pháp gỡ bỏ mã độc trên máy chủ và trong mã nguồn (nếu có);

3. Tăng cường các giải pháp bảo đảm an ninh, an toàn thông tin cho hệ thống

4. Tăng cường các giải pháp bảo đảm an ninh, an toàn thông tin cho các tài khoản cá nhân, tránh tình trạng sử dụng mật khẩu có độ bảo mật yếu, dễ bị chiếm đoạt.

5. Báo cáo kết quả kiểm tra và phương án xử lý về Cục Công nghệ thông tin để theo dõi và làm cơ sở báo cáo lãnh đạo Bộ Y tế và báo cáo Bộ Công an.

Cục Công nghệ thông tin xin trân trọng cảm ơn!

Nơi nhận:
- Như trên;
- Thứ trưởng Lê Quang Cường (để b/c);
- Lưu: VT, CSHT.

PHÓ CỤC TRƯỞNG

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
CỤC CÔNG NGHỆ THÔNG TIN
BỘ Y TẾ

Lương Chí Thành