UBND TỈNH BẾN TRE
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 274 /STTTT-CNTT

V/v hướng dẫn khắc phục lỗ hổng bảo mật nghiêm trọng trên webserver

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

Bến Tre, ngày 11 tháng 5 năm 2012

Kính gửi:
- Các Sở, Ban, Ngành tỉnh;
- Ủy ban nhân dân các huyện, thành phố.

Căn cứ công văn số 97/VNCERT-NCPT ngày 08 tháng 5 năm 2012 của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam về việc thông báo và hướng dẫn khắc phục lỗ hổng bảo mật nghiêm trọng trên máy chủ web, Sở Thông tin và Truyền thông sao gửi đến các cơ quan, đơn vị trên địa bàn tỉnh biết và khắc phục lỗ hổng bảo mật nghiêm trọng trên các webserver.

Trân trọng./.

Nơi nhận:
- Như trên;
- Văn phòng Tỉnh ủy;
- Phòng VHTT các huyện, thành phố;
- Lưu: VT, CNTT (N).

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Ngô Văn Chuyển

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

Số: 97 /VNCERT – NCPT

V/v thông báo và hướng dẫn khắc phục lỗ hổng bảo mật nghiêm trọng trên máy chủ Web.

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

Hà Nội, ngày 08 tháng 05 năm 2012

Kính gửi:

KHẨN

- Các đơn vị chuyên trách về CNTT các Bộ, ngành
- Sở Thông tin và truyền thông các tỉnh, thành phố trực thuộc TW

Trung tâm Ứng cứu khẩn cấp Máy tính Việt Nam (VNCERT) xin thông báo khẩn cấp về lỗ hổng bảo mật rất nguy hiểm (mã số quốc tế : CVE-2012-1823) ảnh hưởng các máy chủ Web(Ví dụ như : Apache, Lighthttpd, Nginx v.v...) cài đặt module PHP-CGI để thực thi các trang web được xây dựng bằng ngôn ngữ PHP qua CGI. Lỗi bảo mật này cho phép tin tặc có thể đánh cắp hoàn toàn mã nguồn, thông tin cấu hình hoặc nguy hiểm hơn có thể cài đặt mã độc, cướp quyền điều khiển các hệ thống máy chủ cài đặt ứng dụng web, Cổng/ Trang thông tin điện tử làm bàn đạp để kiểm soát trái phép hệ thống thông tin nội bộ của các cơ quan, tổ chức.

Để kiểm tra khả năng mắc lỗi bảo mật trên, đề nghị quý đơn vị thực hiện như sau:

1. Mở trình duyệt web
2. Gõ địa chỉ URL như sau: http://tenmien/tentrang.php?-s
   (ví dụ: http://www.vncert.net.vn/index.php?-s)
   Trong đó đơn vị cần điền thông tin về các tham số:
   - **tenmien** – Tên miền của tổ chức
   ví dụ: www.tuoitre.net.vn hoặc www.hoangmai.gov.vn
   - **tentrang** – tên một trang php bất kỳ có trên thư mục public của webserver. Thông thường có thể sử dụng index.php
   - Các từ khóa khác trên địa chỉ giữ nguyên.
3. Hướng dẫn đánh giá kết quả:
   - Nếu trình duyệt web hiện ra toàn bộ mã nguồn của trang php có địa chỉ như đã nêu, thì máy chủ bị lỗi bảo mật trên.
   - Nếu trình duyệt web hiện lên trang web như bình thường thì máy chủ không bị lỗi bảo mật trên.

Hiện nay lỗi bảo mật trên đã được công bố trên diện hẹp tại một số trang thông tin chuyên ngành quốc tế, nên khả năng tin tặc đã biết và có thể lợi dụng để tấn công trái phép vào các hệ thống mắc lỗi bất cứ lúc nào. Trung tâm VNCERT hướng dẫn một số phương án khắc phục như sau:

- Dừng sử dụng phương thức CGI trên máy chủ web server.
- Thay thế module PHP-CGI bằng module Fastcgi.
- Cập nhật phiên bản mới nhất cho các package của php trong webserver, trong đó chú ý hai package **php-common** và **php-cli** từ **Repository** của hệ điều hành cài đặt trên máy chủ web hoặc từ tổ chức PHP tùy vào tình hình thực tế. **Tuy nhiên đề nghị các cơ quan tổ chức chú ý đến ngày 08/5/2012 các bản vá chỉ**

hạn chế được một phần nào, vẫn chưa có bản vá khắc phục được hoàn toàn được lỗi trên cho php-cgi.

Trên đây là ba phương án xử lý do Trung tâm VNCERT đề xuất, tuy nhiên tùy tình hình thực tế cụ thể mà các Quý cơ quan, tổ chức có thể có các biện pháp khắc phục khác phù hợp hơn với thực tế của mình. Do đặc thù lỗ hổng bảo mật trên yêu cầu phải có hiểu biết sâu về hệ thống ứng dụng nên quý cơ quan, tổ chức có thể liên hệ thêm với đơn vị cung ứng phần mềm để có phương án kiểm tra và khắc phục hiệu quả nếu phát hiện lỗi bảo mật.

Theo đánh giá của Trung tâm VNCERT số lượng máy chủ web bị lỗi bảo mật nghiêm trọng trên là khá lớn nên kính đề nghị Quý cơ quan, đơn vị hết sức chú ý, khẩn trương rà soát và thực hiện nghiêm túc theo hướng dẫn trên để ngăn chặn tin tặc khai thác, cướp quyền điều khiển. Hiện nay các thông tin công bố chính thức về lỗi trên đã được các tổ chức quốc tế hạn chế không công bố chi tiết do phạm vi ảnh hưởng rộng, mức độ nghiêm trọng cao mà chưa có hướng khắc phục hoàn chỉnh. Trung tâm VNCERT đang tiếp tục theo dõi và nghiên cứu vấn đề trên, do đó đề nghị Quý cơ quan, tổ chức không công bố thông tin rộng rãi khi nhận được thông báo này. Mọi thắc mắc về việc khắc phục lỗ hổng bảo mật xin liên hệ Thạc sỹ Ngô Quang Huy, Trưởng phòng Kỹ thuật hệ thống - địa chỉ email : traodoiatttt@vncert.vn

Trân trọng thông báo./.

Nơi nhận:
- Như trên;
- Lưu: VT, NCPT, KTHT.

GIÁM ĐỐC

TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

Vũ Quốc Khánh