UBND TỈNH BẾN TRE
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 902/STTTT-CNTT
V/v cảnh báo lỗ hổng bảo mật của phần mềm thư điện tử Zimbra

Bến Tre, ngày 30 tháng 12 năm 2013

SỞ GIÁO DỤC VÀ ĐÀO TẠO BẾN TRE
ĐẾN Số: 11 Ngày: 2/1/14
Chuyển:
Lưu hồ sơ số:

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

Ngày 24 tháng 12 năm 2013, Sở Thông tin và Truyền thông nhận được cảnh báo của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam về lỗ hổng bảo mật nghiêm trọng của phần mềm thư điện tử Zimbra tại công văn số 364/VNCERT-KTHT ngày 18 tháng 12 năm 2013.

Nhằm giảm thiểu tối đa rủi ro mất an toàn, an ninh thông tin của các cơ quan, đơn vị có sử dụng phần mềm thư điện tử Zimbra, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị tiến hành rà soát lại toàn bộ hệ thống và thực hiện các biện pháp kỹ thuật theo hướng dẫn tại văn bản 364/VNCERT-KTHT của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (*đính kèm*).

Thông tin chi tiết xin vui lòng liên hệ:
- Phòng Công nghệ thông tin - Sở Thông tin và Truyền thông.
- Điện thoại: 3.818107 (gặp đ/c Nhã) - Fax: 3.818104.
- Email: nhant@ict-bentre.gov.vn

Trân trọng./.

Nơi nhận:
- Như trên;
- Giám đốc (báo cáo);
- Phòng VHTT các huyện, thành phố;
- Lưu: VT, CNTT.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

SỞ THÔNG TIN VÀ TRUYỀN THÔNG TỈNH BẾN TRE

Trịnh Minh Châu

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

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

Số: 364 /VNCERT- KTHT

Hà Nội, ngày 18 tháng 12 năm 2013

V/v : *Cảnh báo lỗ hổng bảo mật của phần mềm thư điện tử Zimbra*

Kính gửi: Sở Thông tin và Truyền thông Bến Tre

Trung tâm Ứng cứu khẩn cấp Máy tính Việt Nam (VNCERT) xin thông báo tới quý cơ quan về lỗ hổng an toàn thông tin nghiêm trọng của phần mềm thư điện tử Zimbra (TĐT Zimbra). Lỗ hổng này có khả năng cho phép quản trị hoặc khai thác thông tin của hệ thống thư điện tử Zimbra một cách trái phép và được đặt tên quốc tế là "*Privilegie escalation via LFI*". Các phiên bản sau đây của phần mềm TĐT Zimbra bị ảnh hưởng:

- Tất cả các phiên bản kể từ 7.2.2 trở về trước
- Phiên bản 8.01 và 8.02

Qua theo dõi thông tin cảnh báo và công tác thẩm tra, kiểm tra thử nghiệm, Trung tâm VNCERT xác nhận sự tồn tại của một lỗ hổng ATTT nêu trên. Lỗ hổng này có khả năng cho phép tin tặc khai thác được một số tệp tin cấu hình quan trọng trên máy chủ sử dụng phần mềm TĐT Zimbra mà không cần xác thực, đăng nhập vào hệ thống như quy định. Ví dụ điển hình là tin tặc có thể xem nội dung tệp tin "*localconfig.xml*" chứa các thông tin xác thực, đăng nhập vào hệ thống. Các thông tin bí mật này cho phép tin tặc tiếp tục chiếm được quyền quản trị toàn bộ hệ thống thư điện tử nếu có thể kết nối tới cổng quản trị của hệ thống thư điện tử (Cổng mặc định là 7071).

Thông tin về lỗ hổng ATTT này đã được công khai từ ngày 6/12/2013 nên để giảm thiểu tối đa rủi ro an toàn thông tin cho các cơ quan, tổ chức có sử dụng phần mềm TĐT Zimbra, Trung tâm VNCERT khuyến cáo thực hiện biện pháp kỹ thuật sau để hạn chế rủi ro an toàn thông tin:

Bước 1: Rà soát kiểm tra hệ thống thư điện tử đang sử dụng

- Kiểm tra phiên bản của phần mềm thư điện tử Zimbra đang sử dụng.
- Kiểm tra hệ thống TĐT để phát hiện các dấu hiệu xâm nhập trái phép.
- Nếu phát hiện dấu hiệu xâm nhập trái phép thì thực hiện các biện pháp kỹ thuật theo bước 5.

Bước 2: Nâng cao an toàn truy cập đến cổng quản trị máy chủ thư:

- Kiểm tra, bảo đảm các máy tính quản trị hệ thống TĐT phải là các máy tính "sạch" (không bị nhiễm mã độc).
- Thiết lập cấu hình hệ thống (cấu hình tường lửa trên máy chủ thư, tường lửa của hệ thống mạng hoặc thiết bị định tuyến) chỉ cho phép các máy tính quản trị TĐT được kết nối được tới cổng quản trị của máy chủ TĐT.
- Trường hợp cần quản trị máy chủ thư từ bên ngoài: Xem xét việc triển khai các biện pháp kỹ thuật cho phép kết nối từ bên ngoài đến các máy tính quản trị

TĐT ở trên thông qua giao thức bảo mật có cơ chế mã hóa, xác thực và tạo đường ống (ví dụ: VPN tunnel, SSH tunnel v.v...). Không nên cho phép kết nối trực tiếp tới cổng quản trị của máy chủ TĐT từ mạng Internet.

Bước 3: Tiến hành nâng cấp phần mềm TĐT Zimbra đối với các phiên bản bị ảnh hưởng bởi lỗ hổng

- Sao lưu hệ thống thư điện tử hiện tại.
- Nâng cấp phần mềm Zimbra lên phiên bản mới (là các phiên bản không nằm trong các phiên bản bị ảnh hưởng bởi lỗ hổng được nêu trên).

Bước 4: Thường xuyên theo dõi hoạt động của máy chủ thư để phát hiện dấu hiệu bất thường

- Theo dõi các kết nối tới cổng quản trị của máy chủ TĐT từ các máy tính không phải là máy tính có chức năng quản trị.
- Kiểm tra các thông tin trong tệp tin log để theo dõi các hoạt động tạo, xóa hoặc thay đổi trái phép thông tin của các tài khoản, thông tin cấu hình dịch vụ TĐT.

Bước 5: Nếu phát hiện dấu hiệu hệ thống TĐT đã bị lộ thông tin hoặc truy cập trái phép:

- Thiết lập cấu hình máy chủ TĐT để cấm truy cập, đọc thông tin tệp tin *localconfig.xml* từ tất cả các máy tính thông qua kết nối mạng.
- Thay đổi toàn bộ mật khẩu của các tài khoản hợp lệ trên hệ thống dịch vụ TĐT.
- Rà soát và xóa bỏ các tài khoản mà tin tặc có thể tạo ra trên hệ thống TĐT.
- Rà soát sự thay đổi các thông tin cấu hình máy chủ thư, sử dụng cấu hình dự phòng nếu có.
- Thực hiện nâng cấp phần mềm TĐT Zimbra theo bước 3.

Trung tâm VNCERT đề nghị các cơ quan, tổ chức có sử dụng dịch vụ TĐT Zimbra kiểm tra ngay phiên bản phần mềm Zimbra đang sử dụng, nhanh chóng triển khai biện pháp khắc phục và phản hồi thông tin cho Trung tâm VNCERT. Mọi thông tin chi tiết xin vui lòng liên hệ Phòng Kỹ thuật hệ thống/Trung tâm VNCERT, số điện thoại: 0436404424 hoặc email: *antoanthudientu@report.vncert.vn.*

Trân trọng ./.

Nơi nhận:
- Như trên;
- Thứ trưởng Nguyễn Minh Hồng (để b/c)
- Lưu: VT,KTHT.

GIÁM ĐỐC

TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

Vũ Quốc Khánh