UBND TỈNH QUẢNG BÌNH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số:**116**/STTTT-CNTT

V/v cảnh báo điểm yếu mới của hệ quản trị nội dung mã nguồn mở Joomla và hình thức tấn công mới vào các trang tin điện tử tại Việt Nam

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

Quảng Bình, ngày 19 tháng 02 năm 2016

Kính gửi:

- Các Sở, ban, ngành cấp tỉnh;
- UBND các huyện, thị xã, thành phố;
- Các Doanh nghiệp Viễn thông, Công nghệ thông tin.

Trong thời gian gần đây, tại Việt Nam xuất hiện loại hình tấn công bằng cách khóa trang tin điện tử để đòi tiền chuộc, sử dụng hình thức tấn công mã hóa tống tiền (ransomlock). Qua thông tin thu thập được của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT), việc tăng vọt của hình thức tấn công này có liên quan đến điểm yếu của hệ quản trị nội dung Joomla đã được công bố.

Với cách thức tấn công mã hóa trang tin điện tử để đòi tiền chuộc, tin tặc hướng trực tiếp vào người chủ trang tin điện tử, làm cho trang tin điện tử bị tê liệt vì bị mã hóa nội dung và người sở hữu trang tin điện tử phải trả tiền cho tin tặc nếu muốn trang tin điện tử hoạt động trở lại.

1. Tình hình khai thác lỗ hổng và thủ đoạn tấn công mã hoá dữ liệu

Điểm yếu bảo mật mới nhất của Joomla đã được các nhà phát triển Joomla xác nhận có mã là CVE-2015-8562, đây là một điểm yếu Zero-day, với các phiên bản Joomla bị ảnh hưởng là từ V1.5.0 đến V3.4.5. Điểm yếu này cho phép tin tặc thực thi lệnh các đoạn mã độc từ xa với đầy đủ các quyền. Hiện tại Joomla đã ban hành bản vá, tuy nhiên ngay khi điểm yếu này được tiết lộ thì trên Intemet, mã khai thác cũng đã xuất hiện, theo ghi nhận của nhiều tổ chức thì các tấn công khai thác điểm yếu này cũng tăng lên. Mức độ nguy hiểm của điểm yếu này tăng lên khi đã có ghi nhận xu hướng tin tặc thực hiện tấn công nhằm mục đích cài đặt các cửa hậu vào hệ thống trước khi quản trị cập nhật bản vá, chính vì vậy ngay cả cập nhật bản vá, trang tin điện tử vẫn bị tấn công và mã hóa dữ liệu. Ở Việt Nam, cũng đã ghi nhận một số trang tin điện tử bị tấn công

và mã hóa tài liệu với nội dung hiển thị đòi tiền chuộc mà tin tặc để lại trên trang web bị tấn công.

Qua phân tích từ các chuyên gia của VNCERT cho thấy nhiều khả năng khi khai thác thành công lỗ hổng này hay bất kỳ lỗ hổng nào của ứng dụng, tin tặc có thể kiểm soát được toàn bộ nội dung trang tin điện tử. Và việc kiểm soát, tấn công chiếm quyền điều khiển thông qua lỗ hổng, điểm yếu của ứng dụng web hoàn toàn có thể được tin tặc kết hợp thủ đoạn tấn công mã hoá dữ liệu để đòi tiền chuộc từ chủ sở hữu trang tin điện tử.

2. Những nguy cơ tiềm ẩn và trách nhiệm của các tổ chức liên quan

Sự cố tấn công này cho thấy tin tặc đã có xu hướng tấn công từ lợi dụng trang tin điện tử làm bàn đạp sang hình thức tấn công có tính chất phá hoại cao hơn, thêm vào đó việc lợi dụng các điểm yếu Zero-day để tranh thủ khai thác và cài sẵn các cửa hậu cho thấy các loại hình tấn công mạng đã có sự dịch chuyển.

Với các trang tin điện tử bị tấn công theo hình thức này thì các đơn vị, doanh nghiệp sẽ bị mất hết dữ liệu, dẫn đến sẽ phải trả tiền chuộc hoặc xây dựng lại từ đầu các nội dung. Điều này gây thiệt hại cho các nguồn lực của doanh nghiệp và của xã hội.

Việc khai thác điểm yếu của Joomla, một hệ thống quản trị nội dung do chính các nhà cung cấp dịch vụ lưu trữ hoặc đơn vị chịu trách nhiệm quản trị máy chủ, ứng dụng cài đặt, người dùng không thể chủ động cập nhật, do vậy các doanh nghiệp cung cấp dịch vụ lưu trữ hoặc hoặc đơn vị chịu trách nhiệm quản trị máy chủ, ứng dụng phải có trách nhiệm trong việc nhanh chóng vá các lỗ hổng này.

3. Yêu cầu thực hiện

Xét thấy tính chất nghiêm trọng điểm yếu của hệ quản trị nội dung Joomla và xu hướng tấn công mới của tội phạm, Sở Thông tin và Truyền thông yêu cầu các đơn vị thực hiện các công việc sau:

a) Yêu cầu chung

Kiểm tra, rà soát các máy chủ sử dụng hệ quản trị nội dung Joomla đang sử dụng (nếu có) và cập nhật ngay bản vá cho các phiên bản Joomla bị ảnh hưởng.

Chủ động sao lưu dữ liệu cho các máy chủ đặc biệt là các máy chủ web có khả năng bị tấn công, đảm bảo an toàn cho các bản sao lưu, tuyệt đối không để các bản sao lưu dữ liệu trên cùng một máy chủ hoặc trên các máy chủ có kết nối mạng.

Thường xuyên theo dõi, kiểm tra để có phương án xử lý kịp thời khi có các điểm yếu được phát hiện, tiến hành cập nhật các bản vá cũng như đưa ra phương án giảm thiểu thiệt hại trong thời gian sớm nhất.

Tiếp tục thực hiện cảnh báo tới các đơn vị nằm trong phạm vi trách nhiệm và địa bàn hoạt động của đơn vị mình.

b) Yêu cầu đối với các doanh nghiệp cung cấp dịch vụ lưu trữ

Kiểm tra, rà soát các máy chủ sử dụng hệ quản trị nội dung Joomla đang sử dụng (nếu có) và cập nhật ngay bản vá cho các phiên bản Joomla bị ảnh hưởng.

Chủ động sao lưu dữ liệu của các máy chủ hoặc khuyến nghị khách hàng thực hiện sao lưu dữ liệu định kỳ tùy theo mức độ quan trọng của dữ liệu. Tuyệt đối không để các bản dữ liệu sao lưu trên cùng một máy chủ hoặc trên các máy chủ có kết nối mạng.

Thường xuyên theo dõi, kiểm tra để có phương án xử lý kịp thời khi có các điểm yếu được phát hiện, tiến hành cảnh báo cho khách hàng cũng như cập nhật các bản vá hay đưa ra phương án xử lý giảm thiểu thiệt hại trong thời gian sớm nhất.

4. Tổng hợp, báo cáo

Các đơn vị chủ động báo cáo về Sở Thông tin và Truyền thông tình hình xử lý hoặc sự cố tấn công vào các máy chủ của đơn vị và các khó khăn trong việc triển khai các giải pháp đảm bảo an toàn thông tin để xây dựng phương án xử lý kịp thời. Nội dung báo cáo và các khó khăn vướng mắc xin gửi về Sở Thông tin và Truyền thông trước ngày 05/03/2016 theo địa chỉ:

Phòng Ứng cứu sự cố máy tính, Trung tâm Công nghệ thông tin và Truyền thông Quảng Bình

Địa chỉ: 02 Hương Giang - TP.Đồng Hới - Quảng Bình;
Điện thoại: 052.3817456; Email: ungcuusuco@quangbinh.gov.vn.

Trân trọng./.

Nơi nhận:
- GĐ Sở {để báo cáo};
- TT.CNTT-TT;
- Lưu: VT, CNTT.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Nguyễn Phi Khanh