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

Số: 201/VNCERT – KTHT

V/v cảnh báo và đề nghị kiểm tra, xử lý lỗ hổng ATTT trên phần mềm phân giải tên miền BIND

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

Hà Nội, ngày 13 tháng 08 năm 2015

Kính gửi:
- Cơ quan chuyên trách về CNTTT của các Bộ, cơ quan ngang Bộ;
- Sở TT&TT các tỉnh, các thành phố trực thuộc Trung ương.

1. Thông báo về lỗ hổng CVE-2015-5477 trên phần mềm BIND

Phần mềm phân giải tên miền BIND là phần mềm được cài đặt trên các máy chủ sử dụng hệ điều hành Linux để cung cấp dịch vụ phân giải tên miền. Đây là một phần mềm mã nguồn mở, do công ty Internet Systems Consortium Inc (ISC) phát triển và hỗ trợ. Theo các chuyên gia đánh giá thì BIND là phần mềm phân giải tên miền hiện đang được dùng rộng rãi nhất trên thế giới (Theo VNNIC thì chiếm đến trên 70%).

Gần đây, một số phiên bản của phần mềm BIND đã bị phát hiện có lỗ hổng an toàn thông tin (ATTT) cho phép tin tặc tấn công từ xa gây ngưng trệ hoạt động, từ chối dịch vụ (DOS) phân giải tên miền. Với lỗ hổng này, kẻ xấu có thể dễ dàng lợi dụng để tấn công, gây sự cố mất an toàn cho hệ thống thông tin và mạng. Lỗ hổng này đã được nhà sản xuất là công ty ISC chính thức xác nhận vào cuối tháng 7/2015 và đã được MITRE Corporation đặt mã quốc tế là CVE-2015-5477. Cụ thể hơn về lỗ hổng CVE-2015-5477 có thể tham khảo các tài liệu chi tiết tại trang web https://kb.isc.org/article/AA-01272/0.

2. Cảnh báo nguy cơ mất ATTT do lỗ hổng CVE-2015-5477

Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) đã kiểm thử và đánh giá lỗ hổng CVE-2015-5477 có mức nguy hiểm cao và dễ thực hiện. Lỗ hổng này có thể bị tin tặc khai thác để tấn công, gây ra các sự cố ATTT ảnh hưởng nghiêm trọng tới khả năng truy cập các hệ thống thông tin và nhiều dịch vụ, ứng dụng đang được nhiều cơ quan, đơn vị cung cấp. Do vậy, các cơ quan, tổ chức cần có phản ứng kịp thời để phòng ngừa các sự cố ATTT có thể xảy ra.

Lỗ hổng CVE-2015-5477 có ở đâu ?

Kết quả phân tích, đánh giá cho thấy Lỗ hổng CVE-2015-5477 xuất hiện trên phần mềm BIND các phiên bản sau:

- Các phiên bản từ 9.1.0 đến 9.8.x,
- Các phiên bản từ 9.9.0 đến 9.9.7-P1,
- Các phiên bản từ 9.10.0 đến 9.10.2-P2.

Các phần mềm BIND phiên bản nêu trên hiện đang được sử dụng khá phổ biến tại các hệ thống thông tin trọng điểm (Trung tâm hạ tầng CNTT, Trung tâm dữ liệu v.v..) của Tỉnh, Thành phố, Bộ, ngành, đoàn thể Trung ương v.v.

Lỗ hổng CVE-2015-5477 gây ra nguy cơ gì ?

Các ứng dụng, hệ thống thông tin có Lỗ hổng CVE-2015-5477 sẽ có nguy cơ bị tin tặc khai thác, tấn công gây ra các sự cố an toàn thông tin như: ngưng trệ hoạt động, gây tình trạng từ chối dịch vụ phân giải tên miền. Khi xảy ra sự cố an toàn thông tin này sẽ thường làm cho gián đoạn, mất khả năng truy cập vào các ứng dụng và dịch vụ CNTT trực tuyến của cơ quan chủ quản hệ thống tên miền bị tấn công.

Thực tế vừa qua cho thấy, nếu máy chủ dịch vụ phân giải tên miền của một Tỉnh bị sự cố thì thường gây ảnh hưởng, gián đoạn, mất khả năng truy cập các dịch vụ trực tuyến do Tỉnh cung cấp. Trong đó có các hệ thống điển hình như:

- Cổng Thông tin điện tử;
- Hệ thống Thư điện tử;
- Hệ thống dịch vụ Công trực tuyến v.v...

3. Đề nghị xử lý và phối hợp

Do tính chất nguy hiểm của Lỗ hổng CVE-2015-5477, Trung tâm VNCERT đề nghị Lãnh đạo quý cơ quan, tổ chức phối hợp, chỉ đạo thực hiện một số nội dung sau:

1) Chỉ đạo lực lượng ứng cứu khẩn cấp sự cố ATTT, bộ phận kỹ thuật quản trị mạng hoặc bộ phận có chức năng liên quan khẩn trương tiến hành kiểm tra, rà soát ngay hệ thống, ứng dụng của mình và các hệ thống, ứng dụng trong phạm vi, lĩnh vực mình chịu trách nhiệm để phát hiện các hệ thống, ứng dụng có sử dụng phần mềm BIND bị lỗ hổng an toàn thông tin mã số CVE-2015-5477. Chú ý kiểm tra cả các phần mềm BIND đã được cài đặt nhưng không sử dụng.

2) Khi phát hiện có hệ thống, ứng dụng bị Lỗ hổng CVE-2015-5477, cần triển khai ngay việc xử lý, khắc phục, loại bỏ kịp thời lỗ hổng này, tránh để xảy ra các sự cố ATTT đáng tiếc.

3) Gửi báo cáo tình hình, kết quả khắc phục Lỗ hổng CVE-2015-5477 về Trung tâm VNCERT để tổng hợp, báo cáo cấp trên.

Thông tin chi tiết hoặc yêu cầu khác liên quan đến việc xử lý Lỗ hổng CVE-2015-5477 vui lòng liên hệ với đầu mối của VNCERT theo địa chỉ:

Anh Trần Tuấn Anh – Phó Trưởng phòng Kỹ thuật hệ thống

Email : ttanh@vncert.vn Điện thoại: 043.640.44.21 (ext 202)

Trung tâm ứng cứu khẩn cấp máy tính Việt Nam trân trọng cảm ơn sự phối hợp của Quý cơ quan, đơn vị ./.

Nơi nhận:
- Như trên;
- Ban chỉ đạo CNTT các Bộ, ngành, địa phương (để Ph/h);
- Thứ trưởng Nguyễn Thành Hưng (để b/c);
- PGĐ Ngô Quang Huy (để theo dõi);
- Lưu: VT, KTHT, NV.

GIÁM ĐỐC

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

Nguyễn Trọng Đường