UBND TỈNH GIA LAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 338/STTTT-CNTT
V/v cảnh báo nguy cơ bị lây nhiễm mã độc qua lỗ hổng trên phần mềm Winrar chưa cập nhật

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

Gia Lai, ngày 21 tháng 3 năm 2019

Kính gửi:
- Ủy ban Mặt trận Tổ quốc Việt Nam tỉnh;
- Văn phòng Tỉnh ủy;
- Văn phòng UBND tỉnh;
- Văn phòng Đoàn Đại biểu Quốc hội tỉnh;
- Văn phòng Hội đồng nhân dân tỉnh;
- Bộ Chỉ huy Quân sự tỉnh;
- Công an tỉnh;
- Các Sở, ban, ngành;
- Đài Phát thanh - Truyền hình tỉnh;
- Báo Gia Lai;
- Các Hội, Đoàn thể;
- Ủy ban nhân dân các huyện, thị xã, thành phố;
- Các Doanh nghiệp Viễn thông trên địa bàn tỉnh.

Ngày 18/3/2019, Cục An toàn thông tin – Bộ Thông tin và Truyền thông có Công văn số 251/CATTT-NCSC về việc nguy cơ bị lây nhiễm mã độc qua lỗ hổng trên phần mềm Winrar chưa cập nhật *(có bản chụp Công văn kèm theo)*.

Theo đó, Trung tâm Giám sát an toàn thông tin mạng quốc gia (NCSC) thuộc Cục An toàn thông tin (ATTT) thông báo thời gian gần đây, ghi nhận nhiều chiến dịch phát tán mã độc, tấn công mạng thông qua lỗ hổng trên phần mềm **Winrar (CVE 2018-20250).** Lỗ hổng này cho phép đối tượng tấn công cài cắm mã độc vào máy người dùng và ảnh hưởng đến tất cả các phiên bản của Winrar phát hành trong thời gian qua. Hình thức phổ biến để phát tán mã độc được đối tượng tấn công đã thực hiện như sau:

- Lựa chọn những tập tin tài liệu có độ tin cậy cao, thường sử dụng tài liệu của chương trình, hội nghị được nhiều người quan tâm.

- Sử dụng phần mềm Winrar để nén tập tin tài liệu này và tập tin mã độc. Phát tán tập tin nén bằng phần mềm Winrar qua nhiều kênh khác nhau: thư điện tử, hoặc các tập tin tài liệu trên mạng (tài liệu hội nghị, hội thảo...). Người dùng mở tập tin nén này sẽ chỉ nhìn thấy tập tin tài liệu thông thường *(Tham khảo hình ảnh kèm theo trong Công văn số 251/CATTT-NCSC).*

- Khi người dùng giải nén bằng phần mềm **Winrar có chứa lỗ hổng** thì mã độc cũng được giải nén vào thư mục Startup của Windows để thực thi trong lần khởi động tiếp theo của máy tính.

Đặc biệt lỗ hổng này cũng đã được lợi dụng để thực hiện tấn công APT trong sự kiện Hội nghị thượng đỉnh Hoa Kỳ - Triều Tiên để tấn công vào một số cơ quan, tổ chức Việt Nam thực hiện các công tác tổ chức cho sự kiện. Cục ATTT đã cảnh báo nguy cơ tấn công mạng bằng lỗ hổng này thông qua Hệ thống phân tích và chia sẻ nguy cơ tấn công mạng Việt Nam (https://ti.khonggianmang.vn), Bản tin ATTT Tuần 7, Tuần 9/2019.

Trước thực trạng trên cùng với việc Winrar là một trong những phần mềm nén tập tin phổ biến ở Việt Nam nhưng chưa có cơ chế cập nhật tự động, đồng thời nhiều cơ quan tổ chức chưa chú trọng đến công tác rà soát, xử lý các điểm yếu lỗ hổng ATTT. Vì vậy, nhằm bảo đảm an toàn thông tin, phòng tránh các nguy cơ lây nhiễm mã độc thông qua lỗ hổng này, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị, doanh nghiệp thực hiện:

1. Rà soát và kiểm tra phiên bản phần mềm Winrar đang được cài đặt và sử dụng trên toàn bộ máy tính, máy chủ của đơn vị mình;

2. Máy tính, máy chủ nào đang sử dụng các phiên bản cũ cần loại bỏ phần mềm khỏi máy tính; cập nhật lên phiên bản Winrar mới nhất (Winrar 5.7.0). Chú ý chỉ tải phần mềm từ trang chủ Winrar hoặc tổ chức tin cậy. Đường dẫn tài phiên bản Winrar mới nhất*: https://www.win-rar.com/download.html* hoặc *https://www.rarlab.com (Tham khảo hướng dẫn kèm theo).*

Trong trường hợp cần thiết, Quý đơn vị có thể liên hệ với Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), số điện thoại: 0243.209.1616, thư điện tử ais@mic.gov.vn để được hỗ trợ.

3. Khi phát hiện có sự cố hoặc nguy cơ làm mất an toàn, an ninh thông tin phải báo cáo kịp thời về Bộ phận giúp việc của Đội ứng sự cố an toàn thông tin tỉnh (Trung tâm Công nghệ thông tin và Truyền thông Gia Lai) và cùng phối hợp xử lý. Cán bộ đầu mối tiếp nhận, xử lý: Ông Nguyễn Tiến Cường, điện thoại: 02693.512282, di động: 0166.367.5110, Email: cuongnt.stttt@gialai.gov.vn; hoặc Phòng Công nghệ thông tin – Sở Thông tin và Truyền thông, số điện thoại: 02693.719.653 (gặp đồng chí: Nguyễn Thị Ngọc Quyên).

Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị, doanh nghiệp quan tâm thực hiện./.

Nơi nhận:
- Như trên;
- UBND tỉnh (báo cáo);
- Trung tâm CNTT&TT (thực hiện);
- Lưu: VT, P.CNTT.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Đặng Quang Khanh