UBND TỈNH GIA LAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 1148/STTTT-CNTT
V/v cảnh báo lỗ hổng bảo mật mới trong phần mềm WinRAR

Gia Lai, ngày 13 tháng 7 năm 2021

Kính gửi:
- Công an tỉnh;
- Bộ Chỉ huy Quân sự tỉnh;
- Bộ Chỉ huy Bộ đội biên phòng tỉnh;
- Văn phòng Tỉnh ủy;
- Văn phòng Hội đồng nhân dân tỉnh;
- Văn phòng Ủy ban Mặt trận tổ quốc Việt Nam tỉnh;
- Các sở, ban, ngành thuộc tỉnh;
- Các hội, đoàn thể tỉnh;
- Ủy ban nhân dân các huyện, thị xã, thành phố;
- Trung tâm CNTT&TT tỉnh Gia Lai.

Ngày 02/7/2021, qua công tác giám sát trên không gian mạng, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin đã ghi nhận điểm yếu, lỗ hổng bảo mật mới (CVE-2021-35052) trong phần mềm WinRAR.

Phần mềm WinRAR là công cụ hỗ trợ người dùng trong việc nén và giải nén các tệp tin. Theo đánh giá sơ bộ, đây là lỗ hổng có phạm vi ảnh hưởng tương đối lớn, do phần mềm WinRAR được sử dụng phổ biến hiện nay trong các cơ quan tổ chức cũng như người dùng cá nhân. Khai thác thành công lỗ hổng này, đối tượng tấn công có thể thực hiện tấn công vào hàng loạt các máy tính người dùng đang sử dụng phần mềm WinRAR, từ đó có thể dẫn đến các chiến dịch tấn công có chủ đích trên diện rộng.

Thực hiện khuyến nghị của Cục An toàn thông tin tại Công văn số 861/CATTT-NCSC ngày 05/7/2021 về việc lỗ hổng bảo mật mới trong WinRAR; Sở Thông tin và Truyền thông tỉnh Gia Lai đề nghị các đơn vị, địa phương có sử dụng máy tính đang sử dụng phần mềm WinRAR, khắc phục kịp thời lỗ hổng bảo mật mới (CVE-2021-35052), cụ thể như sau:

1. Kiểm tra, rà soát máy tính đang sử dụng phần mềm WinRAR có khả năng bị ảnh hưởng bởi lỗ hổng bảo mật mới (CVE-2021-35052) để có phương án xử lý, khắc phục lỗ hổng kịp thời. Cập nhật lên phiên bản mới nhất (hiện tại là **6.02**) theo phát hành của hãng phần mềm (*hướng dẫn chi tiết trong Phụ lục đính kèm*)

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng.

Sở Thông tin và Truyền thông tỉnh Gia Lai đề nghị các đơn vị, địa phương phối hợp, triển khai thực hiện./.

Nơi nhận:
- Như trên;
- UBND tỉnh (báo cáo);
- Cục An toàn thông tin (báo cáo);
- Lưu: VT, P. CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Đặng Quang Khanh

Phụ lục:

THÔNG TIN VỀ LỖ HỔNG BẢO MẬT MỚI TRONG PHẦN MỀM WINRAR VÀ HƯỚNG DẪN XỬ LÝ, KHẮC PHỤC LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số : 1148/STTTT-CNTT ngày 13 tháng 7 năm 2021 của Sở Thông tin và Truyền thông tỉnh Gia Lai)

1. Thông tin các lỗ hổng bảo mật:

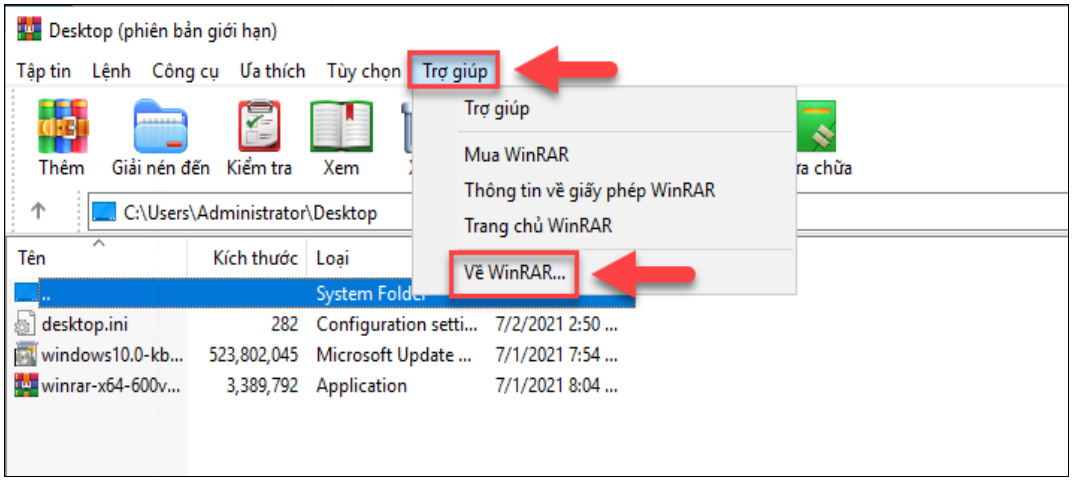
Lỗ hổng bảo mật CVE-2021-35052 tồn tại trong phần mềm WinRAR phiên bản từ 6.01 trở xuống, sử dụng kết nối không an toàn khi truy cập nội dung thông báo từ phía máy chủ của WinRAR thông qua web notifier window của ứng dụng này, dẫn đến có thể khai thác để thay đổi nội dung truyền từ máy chủ bằng cách can thiệp vào được dữ liệu trên đường truyền Internet hoặc thay đổi vào bản ghi DNS. Khai thác lỗ hổng trên, kẻ tấn công thông qua WinRAR có thể thực thi một tệp tin với đường dẫn bất kỳ, từ đó có thể chiếm quyền điều khiển máy tính của người dùng.

2. Hướng dẫn khắc phục:

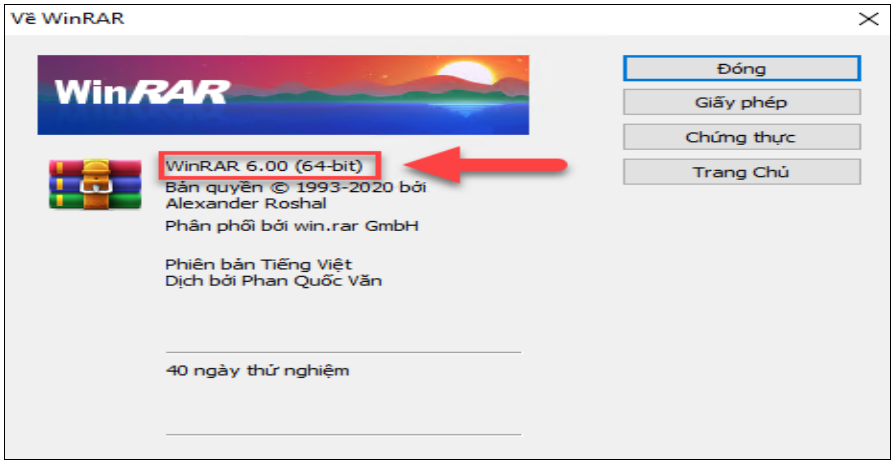
Để khắc phục lỗ hổng, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) khuyến nghị nên thực hiện cập nhật phần mềm WinRAR phiên bản mới nhất (hiện tại là **6.02**) để hạn chế tấn công.

- ***Bước 1***: Kiểm tra phiên bản phần mềm hiện tại đang sử dụng

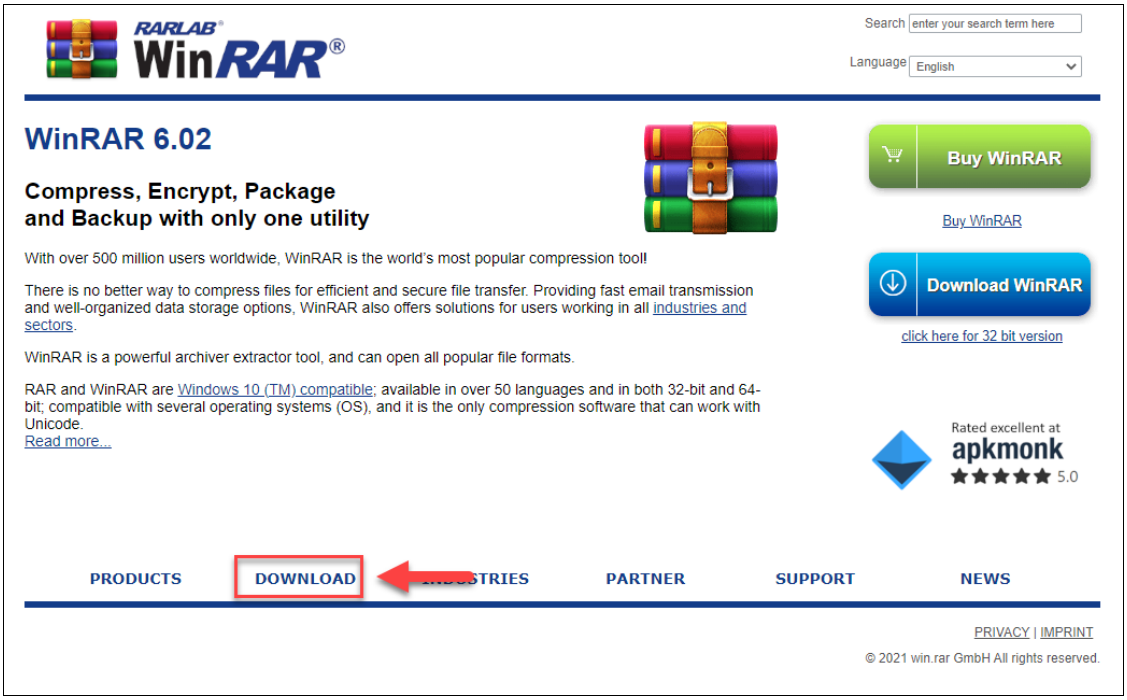
+ Vào mục ***Trợ giúp (Help) > Về WinRAR (about WinRAR)***



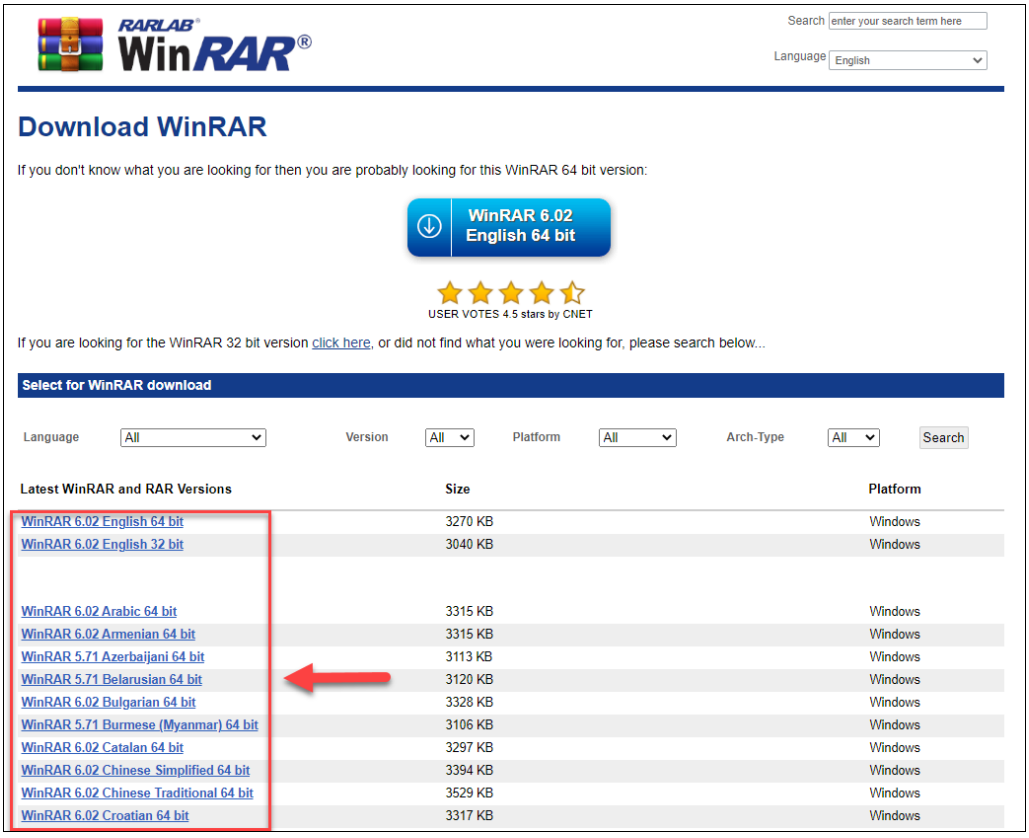
+ Tại cửa sổ pop-up hiển thị thông tin phiên bản WinRAR



- ***Bước 2***: Nếu phiên bản phần mềm hiện tại chưa phải mới nhất (WinRAR 6.02), truy cập *https://www.win-rar.com/*, vào mục ***Download*** để tải phiên bản cao nhất

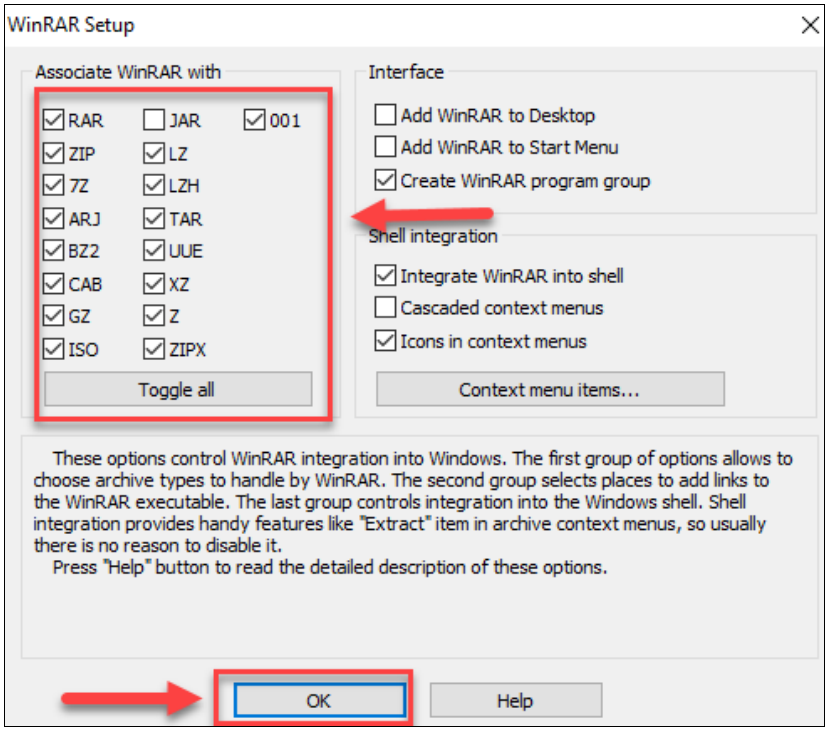


+ Chọn phiên bản mới nhất, phù hợp với hệ điều hành (64/32bit), ngôn ngữ (Tiếng Anh, …) cần tải về:

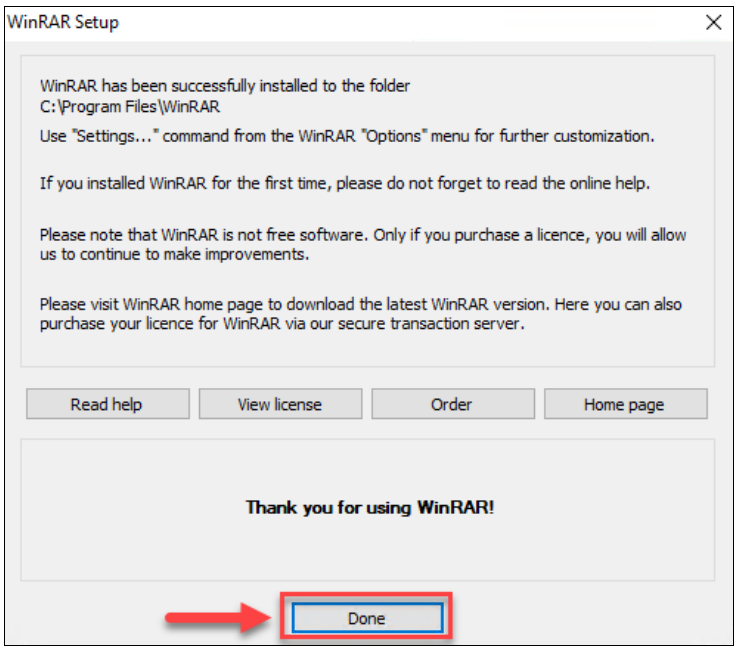


- ***Bước 3*:** Mở bộ cài vừa tải về, chọn ***Install*** để cài đặt

- ***Bước 4*:** Thiết lập chọn các định dạng để WinRAR hỗ trợ sử dụng, chọn ***OK*** để hoàn thành



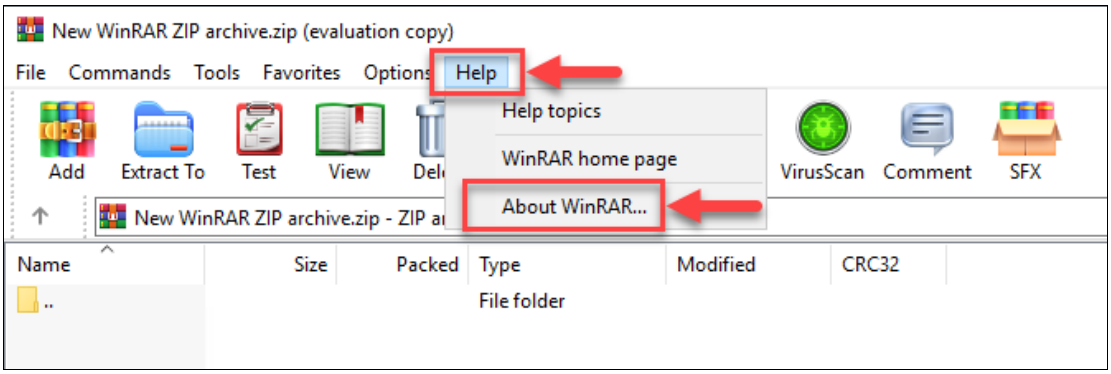
- ***Bước 5*:** Chọn ***Done*** để hoàn thành



- ***Bước 6***: Kiểm tra lại phiên bản phần mềm vừa cài đặt:

+ Mục đích để kiểm tra phần mềm đã được cập nhật, cài đặt thành công hay chưa

+ Thực hiện lại **B1** để kiểm tra lại phiên bản phần mềm



+ Phần mềm đã cập nhật phiên bản mới nhất tại thời điểm hiện tại (WinRAR 6.02)

3. Tài liệu tham khảo

https://www.winrar.com/singlenewsview.html?L=0&tx_ttnews%5Btt_news%5D=165&cHash=1