BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Số: 180 /TTCNTT-KTHT
V/v lỗ hổng bảo mật mới trong WinRAR

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

Hà Nội, ngày 09 tháng 07 năm 2021

Kính gửi: Các đơn vị trực thuộc Bộ

Ngày 02/07/2021, Cục An toàn thông tin đã ghi nhận điểm yếu, lỗ hổng bảo mật mới **(CVE-2021-35052)** trong phần mềm WinRAR. 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 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 WinRAR, từ đó có thể dẫn đến các chiến dịch tấn công có chủ đích trên diện rộng.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, Trung tâm Côn nghệ thông tin khuyến nghị Quý đơn vị thông báo rộng rãi đến toàn thể cán bộ và thực hiện:

1. Kiểm tra, rà soát máy tính đang sử dụng WinRAR có khả năng bị ảnh hưởng bởi lỗ hổng trên để có phương án xử lý, khắc phục lỗ hổng. Cập nhật lên phiên bản mới nhất **(hiện tại là 6.02)** theo phát hành của hãng (tham khảo hướng dẫn kèm theo).

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

Trong trường hợp cần thiết, Quý đơn vị liên hệ đầu mối hỗ trợ của Trung tâm Công nghệ thông tin: Phòng Kỹ thuật hạ tầng, điện thoại 024.39439060, thư điện tử: phongktht@most.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Bùi Thế Duy (để b/c);
- Cổng thông tin điện tử Bộ KH&CN;
- Lưu: VT, KTHT.

GIÁM ĐỐC

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Hà Quốc Trung

Phụ lục
Thông tin lỗ hổng bảo mật
(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2021 của Trung tâm Công nghệ thông tin)

1. Thông tin về các lỗ hổng

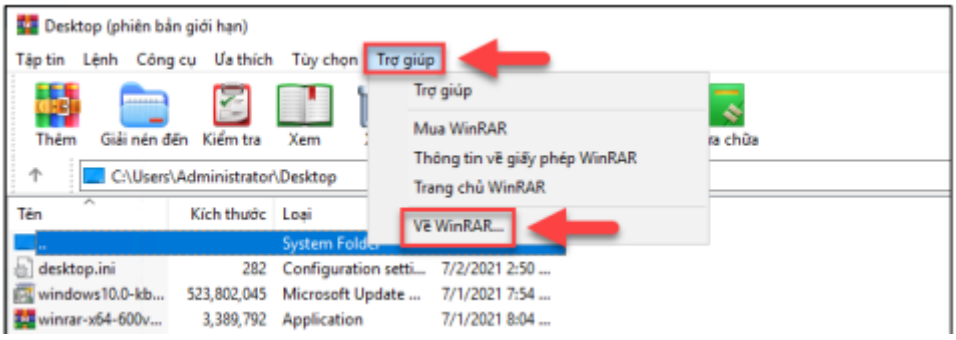
Lỗ hổng bảo mật CVE-2021-35052 tồn tại do các phần mềm WinRAR phiên bản bị ảnh hưởng (từ phiên bản 6.01 trở xuống) sử dụng kết nối không an toàn khi truy cập nội dung thông báo từ phía máy chủ của WinRAR thông qua web notifier window của ứng dụng này, dẫn đến có thể khai thác để thay đổi nội dung truyền 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

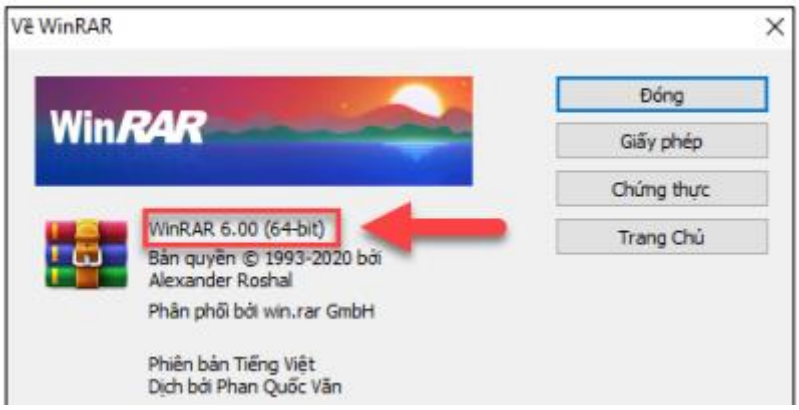
Để khắc phục lỗ hổng, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) khuyến nghị nên thực hiện cập nhật phiên bản mới nhất **(hiện tại là 6.02)** của phần mềm để hạn chế tấn công.

- B1: Kiểm tra phiên bản phần mềm hiện tại đang sử dụng

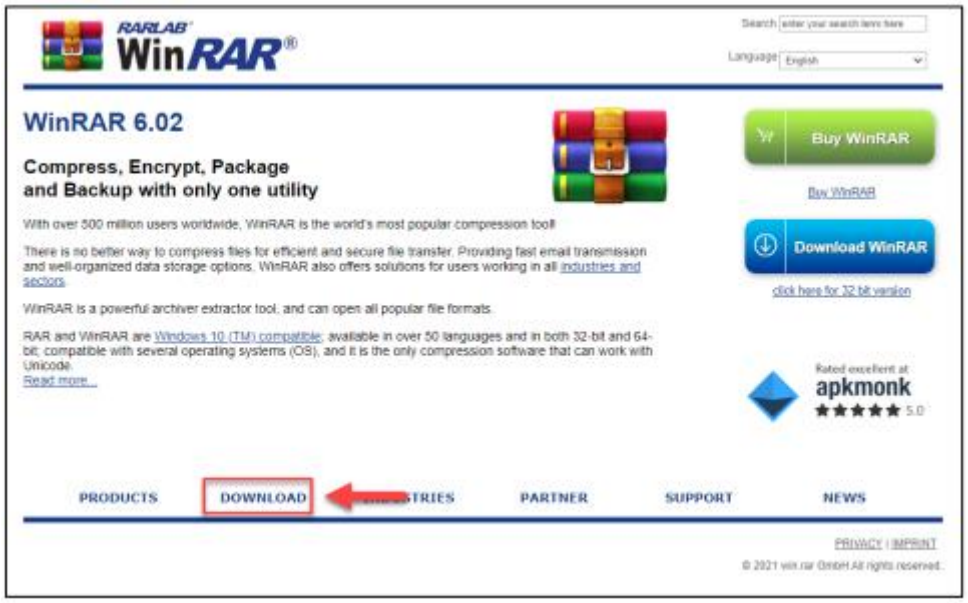
+ Vào mục ***Trợ giúp (Help) > Về WinRAR (about WinRAR)***



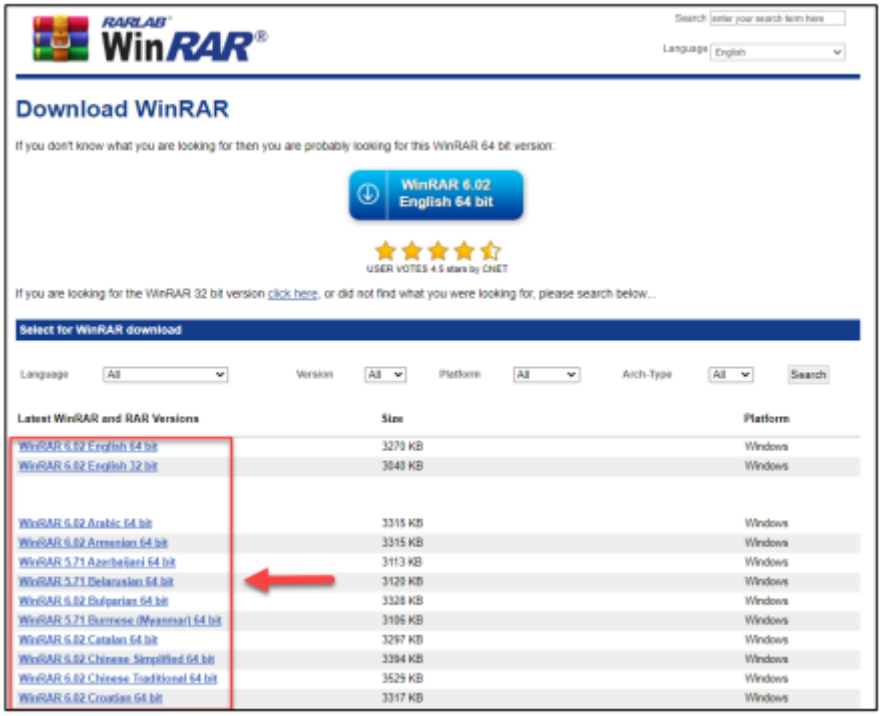
+ Tại cửa sổ pop-up hiển thị thông tin phiên bản WinRAR



- **B2**: 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

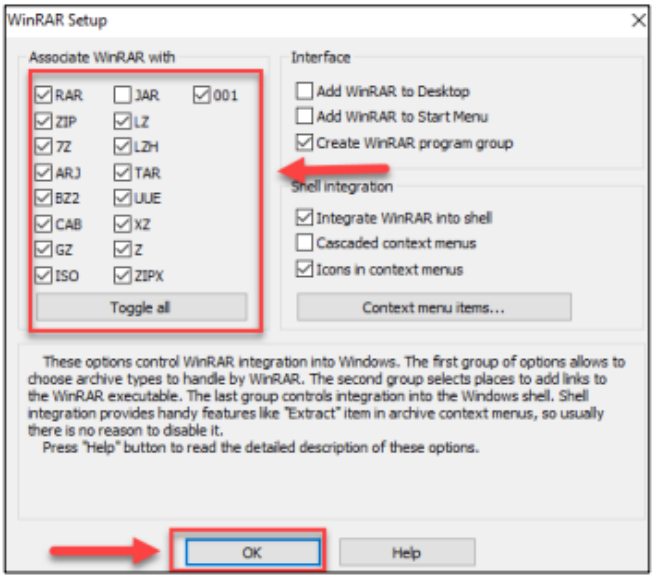


+ Chọn phiên bản mới nhất, phù hợp với hệ điều hành (64/32bit), ngôn ngữ (Tiếng Anh, …) cần tải về:

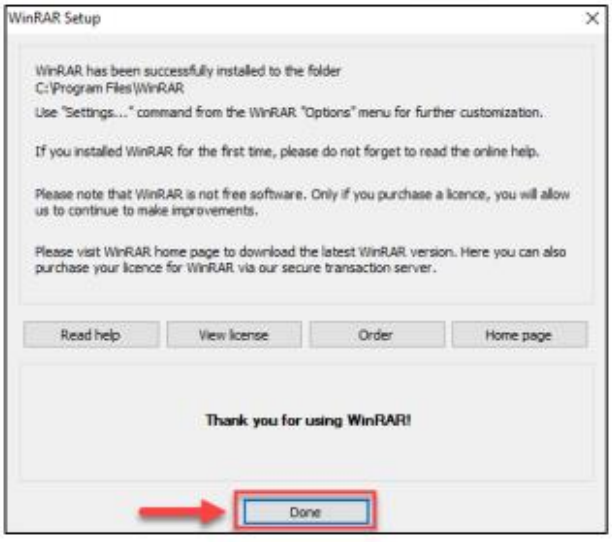


- **B3:** Mở bộ cài vừa tải về, chọn ***Install*** để cài đặt

- B4: Thiết lập chọn các định dạng để WinRAR hỗ trợ sử dụng, chọn ***OK*** để hoàn thành



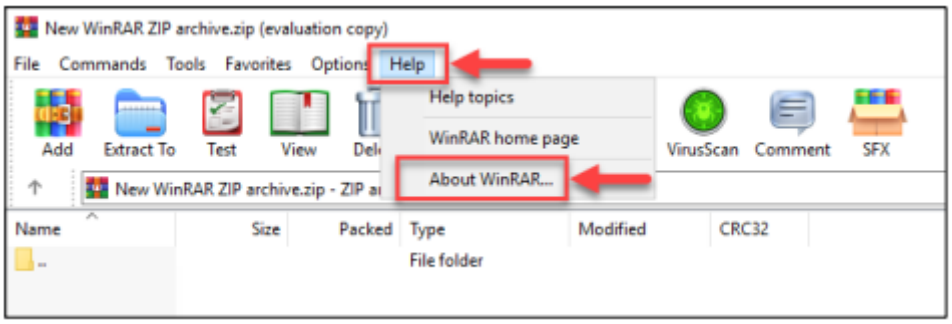
- B5: Chọn ***Done*** để hoàn thành



- **B6**: 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.win-rar.com/singlenewsview.html?L=0&tx_ttnews[tt_news]=165&cHash=1

DANH SÁCH CÁC ĐƠN VỊ CÓ HỆ THỐNG CNTT

(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2021 của Trung tâm Công nghệ thông tin)

TT	Tên đơn vị
1.	Vụ Khoa học Xã hội, Nhân văn và Tự nhiên
2.	Vụ Khoa học và Công nghệ các ngành kinh tế - kỹ thuật
3.	Vụ Đánh giá, Thẩm định và Giám định công nghệ
4.	Vụ Công nghệ cao
5.	Vụ Kế hoạch -Tài chính
6.	Vụ Pháp chế
7.	Vụ Tổ chức cán bộ
8.	Vụ Hợp tác quốc tế
9.	Vụ Thi đua - Khen thưởng
10.	Vụ Phát triển khoa học và công nghệ địa phương
11.	Văn phòng Bộ
12.	Thanh tra Bộ
13.	Cục Công tác phía Nam
14.	Cục Ứng dụng và phát triển công nghệ
15.	Cục Năng lượng nguyên tử
16.	Cục Thông tin Khoa học và Công nghệ Quốc gia
17.	Cục Phát triển thị trường và doanh nghiệp khoa học và công nghệ
18.	Cục An toàn bức xạ và hạt nhân
19.	Cục Sở hữu trí tuệ
20.	Tổng Cục tiêu chuẩn đo lường chất lượng
21.	Ban quản lý khu công nghệ cao Hoà Lạc
22.	Học viện Khoa học, Công nghệ và Đổi mới sáng tạo`
23.	Viện Khoa học và công nghệ Việt Nam - Hàn Quốc (VKIST)
24.	Viện Nghiên cứu sáng chế và Khai thác công nghệ
25.	Viện Năng lượng nguyên tử Việt Nam
26.	Viện Ứng dụng công nghệ
27.	Viện Đánh giá khoa học và Định giá công nghệ
28.	Viện Khoa học sở hữu trí tuệ
29.	Viện Nghiên cứu và Phát triển Vùng
30.	Văn phòng các Chương trình trọng điểm cấp nhà nước
31.	Văn phòng Công nhận chất lượng
32.	Văn phòng Đăng ký hoạt động khoa học và công nghệ
33.	Văn phòng các Chương trình khoa học và công nghệ quốc gia
34.	Báo Khoa học và Phát triển
35.	Tạp chí Khoa học và Công nghệ Việt Nam
36.	Nhà xuất bản Khoa học và Kỹ thuật
37.	Quỹ Phát triển khoa học và công nghệ quốc gia
38.	Quỹ Đổi mới công nghệ quốc gia
39.	Trung tâm Nghiên cứu và Phát triển truyền thông khoa học và công nghệ
40.	Trung tâm Nghiên cứu và Phát triển hội nhập khoa học và công nghệ quốc tế