BỘ TƯ PHÁP
CỤC CÔNG NGHỆ THÔNG TIN

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

Số: 343/CNTT-HTKT&ATTT
V/v Cảnh báo các lỗ hổng bảo mật

Hà Nội, ngày 16 tháng 7 năm 2021

Kính gửi: - Các đơn vị thuộc Bộ Tư pháp;
- Cục Thi hành án dân sự các tỉnh, thành phố trực thuộc Trung ương;
- Sở Tư pháp các tỉnh, thành phố trực thuộc Trung ương.

Hiện nay, tình hình an toàn an ninh thông tin trong nước đang có diễn biến phức tạp, các đơn vị chuyên trách về an toàn an ninh thông tin liên tục đưa ra các cảnh báo, khuyến nghị về công tác đảm bảo an toàn an ninh thông tin trong giai đoạn hiện nay. Thời gian gần đây các chuyên gia bảo mật đã phát hiện nhiều lỗ hổng bảo mật cho phép đối tượng tấn công leo thang đặc quyền, cụ thể:

1. Lỗ hổng bảo mật **(CVE-2021-1675, CVE-2021-31527)** được đánh giá có mức độ nguy hiểm cao ảnh hưởng hầu hết các phiên bản của hệ điều hành Windows *(Windows 10/8.1/7, Windows Server 2021/2016/2012/2008)*. Lỗ hổng này không chỉ cho phép đối tượng tấn công khai thác các thông tin máy tính khi có quyền truy cập trực tiếp vào máy tính/ máy chủ cài đặt phiên bản hệ điều hành bị ảnh hưởng, mà còn có thể tấn công thông qua một máy tính trong mạng. Lỗ hổng này hoàn toàn có thể được tận dụng để tiến hành các chiến dịch tấn công có chủ đích (APT) trên quy mô rộng.

2. Lỗ hổng bảo mật **(CVE-2021-35052)** trong phần mềm WinRAR *(WinRAR là phần mềm công cụ hỗ trợ người dùng trong việc nén và giải nén các tệp tin)*. Theo đánh giá của các chuyên gia bảo mật, 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 (APT) trên diện rộng

3. Lỗ hổng bảo mật **(CVE-2021-21571, CVE-2021-21572, CVE-2021-21573, CVE-2021-21574)** trong tính năng BIOSConnect và HTTPS Boot *(tính năng, công cụ có sẵn để hỗ trợ việc cập nhật firmware và khôi phục hệ điều hành từ xa)* trên BIOS của máy tính, thiết bị hãng Dell. Theo đánh giá sơ bộ, đây là những lỗ hổng có phạm vi ảnh hưởng tương đối lớn, đến khoảng 30 triệu thiết bị tương ứng với 129 dòng máy tính xách tay, máy tính bảng và máy tính bàn. Đặc biệt 04 lỗ hổng này có thể kết hợp với nhau trong các chiến dịch tấn công

có chủ đính để tấn công, kiểm soát máy tính, thiết bị của người dùng, từ đó tấn công sâu hơn vào các hệ thống thông tin quan trọng.

Nhằm bảo đảm an toàn thông tin và phòng tránh nguy cơ bị tấn công có chủ đích (APT), Cục Công nghệ thông tin đề nghị Quý đơn vị thực hiện một số nội dung, cụ thể:

1. Kiểm tra, rà soát và xác định máy chủ, máy trạm sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng. Thực hiện cập nhật bản vá bảo mật cho các máy bị ảnh hưởng theo hướng dẫn của Microsoft.

2. 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 bả mới nhất theo phát hành của hãng.

3. Kiểm tra, rà soát máy tính, thiết bị có khả năng bị ảnh hưởng bởi các lỗ hổng để có phương án xử lý, khắc phục kịp thời. Cập nhật bản vá tương ứng theo phát hành của Dell. Trong trường hợp chưa có bản vá cần có phương án ngăn chặn việc khai thác lỗ hổng, đồng thời theo dõi thường xuyên thông tin về lỗ hổng để cập nhật khi có bản vá.

Tham khảo Hướng dẫn chi tiết tại mục Thông tin điều hành/Thông tin cần lưu ý trên Cổng thông tin điện tử Bộ Tư pháp: *https://moj.gov.vn*.

Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục Công nghệ thông tin, cụ thể: Phòng Hạ tầng kỹ thuật và an toàn thông tin – Cục Công nghệ thông tin, điện thoại: 024.62739717, Email: csht@moj.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Nguyễn Khánh Ngọc (để b/c);
- Lưu: VT.

CỤC TRƯỞNG

CỘNG HÒA XHCN VIỆT NAM
CỤC CÔNG NGHỆ THÔNG TIN
BỘ TƯ PHÁP

Nguyễn Tiến Dũng