

Phụ lục VIII
Quy trình quản lý điểm yếu an toàn thông tin
(Kèm theo Quyết định số /QĐ-BNV ngày /2024
của Bộ trưởng Bộ Nội vụ)

Bước 1: Xác định các thành phần có trong hệ thống có khả năng tồn tại điểm yếu an toàn thông tin (thiết bị hệ thống, hệ điều hành, máy chủ, ứng dụng, dịch vụ và các thành phần khác).

Bước 2: Rà quét các điểm yếu có trong hệ thống (tiến hành rà quét 03 tháng 01 lần)

Bằng các phần mềm chuyên dụng như: Acunetix, Nessus, Tenable,...

Bước 3: Phân loại, xử lý điểm yếu có trong hệ thống

Mức độ nguy hiểm	Mô tả	Xử lý
Nghiêm trọng	Là những điểm yếu khi bị khai thác cho phép tin tặc thực thi lệnh điều khiển mà không cần bất kỳ tác động nào của người sử dụng. Ví dụ: điểm yếu cho phép lây nhiễm mã độc hoặc thực hiện các lệnh điều khiển trên máy tính từ xa mà không đưa ra bất cứ thông báo nào cho người đang sử dụng máy tính.	Khi phát hiện có điểm yếu này thì người sử dụng cần có ngay biện pháp khắc phục hoặc cài đặt bản vá (Patch) do nhà sản xuất phần mềm cung cấp chính thức để ngăn chặn khả năng tin tặc khai thác điểm yếu.
Cao	Là những điểm yếu khi bị khai thác có thể gây ảnh hưởng đến: tính bí mật, toàn vẹn, sẵn sàng đối với dữ liệu của người sử dụng hoặc tài nguyên khác của hệ thống. Những điểm yếu này chỉ bị khai thác khi người sử dụng cố tình bỏ qua những cảnh báo của hệ điều hành hay ứng dụng. Ví dụ: người sử dụng truy cập vào những trang web có chứa mã độc được nhúng trong một đoạn Java Script mặc dù đã được trình duyệt cảnh báo.	Khi phát hiện các điểm yếu loại này người sử dụng cần có biện pháp khắc phục sớm nhất có thể. Trong trường hợp thực hiện nâng cấp hoặc cài đặt bản vá cho các ứng dụng người sử dụng cần xem xét mức độ ảnh hưởng của việc nâng cấp hoặc cài đặt tới các phần mềm và ứng dụng có liên quan.
Trung bình	Là những điểm yếu khi bị khai thác, ảnh hưởng xấu của nó có thể được hạn chế hay khắc phục bằng cách áp dụng biện pháp xác thực hoặc đôi khi chỉ là thay đổi cấu	Khi phát hiện các điểm yếu loại này người sử dụng chỉ thực hiện khi việc nâng cấp hay cài đặt bản vá khi đã xác định rõ bản vá không có ảnh hưởng tới các

	hình mặc định của hệ điều hành, hoặc ứng dụng liên quan đến điểm yếu.	phần mềm, ứng dụng và hệ thống khác liên quan đang hoạt động. Khi chưa cập nhật bản vá hoặc nâng cấp theo hướng dẫn, thì cần có biện pháp bảo vệ và phòng ngừa các sự cố có thể xảy ra theo cảnh báo.
Thấp	Là những điểm yếu khi bị khai thác, ảnh hưởng của nó có thể khắc phục bằng cách thiết lập các thông số của hệ điều hành hoặc ứng dụng bị ảnh hưởng bởi điểm yếu.	Đối với các điểm yếu ở mức nguy hiểm này, việc lựa chọn các biện pháp khắc phục cũng giống như việc lựa chọn các biện pháp khắc phục đối với các điểm yếu có mức độ nguy hiểm Trung bình.

Bước 4: Lập báo cáo các điểm yếu của hệ thống đã xử lý, điểm yếu còn tồn tại trong hệ thống.