MỘT SỐ DẠNG LỖ HỔNG TRONG HỆ ĐIỀU HÀNH VÀ PHẦN MỀM ỨNG DỤNG

Trịnh Thị Vân
Khoa CNTT, Trường Đại học Hạ Long

Tóm tắt: *Trong những năm gần đây, cùng với quá trình đẩy mạnh ứng dụng công nghệ thông tin và chuyển đổi số trong giáo dục, hệ điều hành và các phần mềm ứng dụng đã trở thành công cụ không thể thiếu trong hoạt động dạy học, quản lý và nghiên cứu tại các cơ sở giáo dục. Tuy nhiên, thực tế cho thấy nhiều hệ điều hành và phần mềm ứng dụng vẫn tồn tại các lỗ hổng bảo mật, tiềm ẩn nguy cơ mất an toàn thông tin, ảnh hưởng đến hiệu quả khai thác, sử dụng thiết bị và hệ thống công nghệ trong nhà trường.Việc nhận diện và hiểu rõ các dạng lỗ hổng trong hệ điều hành và phần mềm ứng dụng có ý nghĩa quan trọng, góp phần nâng cao nhận thức về an toàn thông tin cho đội ngũ cán bộ quản lý, giảng viên, giáo viên và người học. Trên cơ sở đó, bài viết tập trung trình bày một số dạng lỗ hổng thường gặp, phân tích nguyên nhân và tác động của chúng, nhằm góp phần đề xuất các giải pháp sử dụng thiết bị và phần mềm an toàn, hiệu quả, đáp ứng yêu cầu đổi mới giáo dục trong giai đoạn hiện nay.*

Từ khoá: *An toàn thông tin; lỗ hổng bảo mật; hệ điều hành; phần mềm ứng dụng; giáo dục số.*

SOME TYPES OF VULNERABILITIES IN OPERATING SYSTEMS AND APPLICATION SOFTWARE

Abstract: *In recent years, along with the accelerated application of information technology and digital transformation in education, operating systems and application software have become indispensable tools in teaching, management, and research activities at educational institutions. However, reality shows that many operating systems and application software still have security vulnerabilities, posing a potential risk of information insecurity and affecting the efficiency of exploiting and using technology equipment and systems in schools. Identifying and understanding the types of vulnerabilities in operating systems and application software is crucial, contributing to raising awareness of information security among administrators, lecturers, teachers, and students. Based on this, the article focuses on presenting some common types of vulnerabilities, analyzing their causes and impacts, in order to contribute to proposing solutions for the safe and effective use of equipment and software, meeting the requirements of educational reform in the current period.*

Keywords: *Information security; security vulnerabilities; operating systems; application software; digital education.*

Nhận bài: 06/03/2026 Phản biện: 23/03/2026 Duyệt đăng: 27/03/2026

I. ĐẶT VẤN ĐỀ

Trong quá trình đẩy mạnh chuyển đổi số và đổi mới phương pháp dạy học, các cơ sở giáo dục ngày càng tăng cường ứng dụng hệ điều hành và phần mềm ứng dụng trong quản lý, giảng dạy và học tập. Nhiều thiết bị giáo dục hiện đại như máy tính, phòng học thông minh, hệ thống học tập trực tuyến, phần mềm quản lý đào tạo… đều hoạt động dựa trên nền tảng của hệ điều hành và phần mềm ứng dụng. Vì vậy, việc bảo đảm an toàn và ổn định cho các hệ thống này là yêu cầu quan trọng nhằm nâng cao hiệu quả sử dụng thiết bị giáo dục.

Tuy nhiên, thực tế triển khai cho thấy nhiều hệ điều hành và phần mềm ứng dụng hiện nay vẫn tồn tại các lỗ hổng bảo mật. Những lỗ hổng này có thể phát sinh trong quá trình thiết kế, lập trình, cài đặt hoặc sử dụng, tạo điều kiện cho các hành vi truy cập trái phép, làm mất dữ liệu hoặc gián đoạn hoạt động của hệ thống. Đối với môi trường giáo dục, các sự cố liên quan đến lỗ hổng phần mềm không chỉ ảnh hưởng đến hoạt động dạy học mà còn gây khó khăn trong công tác quản lý, khai thác và bảo vệ thiết bị giáo dục.

Trong bối cảnh các cơ sở giáo dục ngày càng phụ thuộc vào hệ thống công nghệ và thiết bị số, việc nhận diện các dạng lỗ hổng trong hệ điều hành và phần mềm ứng dụng là cần thiết. Điều này giúp cán bộ quản lý, giáo viên và nhân viên kỹ thuật có cái nhìn tổng quan, từ đó sử dụng và quản lý thiết bị giáo dục một cách an toàn, hiệu quả hơn.

Xuất phát từ thực tiễn trên, bài viết tập trung trình bày các dạng lỗ hổng thường gặp trong hệ điều hành và phần mềm ứng dụng, phân tích ảnh hưởng của các lỗ hổng này đối với việc sử dụng thiết bị giáo dục, đồng thời góp phần nâng cao nhận thức về an toàn thông tin trong các cơ sở giáo dục hiện nay.

II. NỘI DUNG NGHIÊN CỨU

Các dạng lỗ hổng bảo mật thường gặp trong hệ điều hành và các phần mềm ứng dụng bao gồm: Lỗi tràn bộ đệm (Buffer overflows); Lỗi không kiểm tra đầu vào (Unvalidated input); các vấn đề với điều khiển truy nhập (Access-control problems); các điểm yếu trong xác thực, trao quyền hoặc

các hệ mật mã (Weaknesses in authentication, authorization or cryptographic practices); Các lỗ hổng bảo mật khác.

2.1. Lỗi tràn bộ đệm

Lỗi tràn bộ đệm (Buffer overflow) là một trong các lỗi thường gặp trong các hệ điều hành và đặc biệt nhiều ở các phần mềm ứng dụng. Lỗi tràn bộ đệm xảy ra khi một ứng dụng cố gắng ghi dữ liệu vượt khỏi phạm vi của bộ nhớ đệm, là giới hạn cuối hoặc cả giới hạn đầu của bộ đệm. Lỗi tràn bộ đệm có thể khiến ứng dụng ngừng hoạt động, gây mất dữ liệu hoặc thậm chí giúp kẻ tấn công chèn, thực hiện mã độc để kiểm soát hệ thống. Lỗi tràn bộ đệm chiếm một tỷ lệ lớn trong số các lỗi gây lỗ hổng bảo mật. Tuy nhiên, trên thực tế không phải tất cả các lỗi tràn bộ đệm đều có thể bị khai thác bởi kẻ tấn công.

Lỗi tràn bộ đệm xuất hiện trong khâu lập trình phần mềm (coding), trong quy trình phát triển phần mềm. Nguyên nhân của lỗi tràn bộ đệm là người lập trình không kiểm tra, hoặc kiểm tra không đầy đủ các dữ liệu đầu vào nạp vào bộ nhớ đệm. Khi dữ liệu có kích thước quá lớn hoặc có định dạng sai được ghi vào bộ nhớ đệm, nó sẽ gây tràn và có thể ghi đè lên các tham số thực hiện chương trình, có thể khiến chương trình bị lỗi và ngừng hoạt động. Một nguyên nhân bổ sung khác là việc sử dụng các ngôn ngữ với các thư viện không an toàn, như hợp ngữ, C và C++.

Phòng chống

Để phòng chống lỗi tràn bộ đệm một cách hiệu quả, cần kết hợp nhiều biện pháp. Các biện pháp có thể thực hiện bao gồm:

Kiểm tra thủ công mã nguồn hay sử dụng các công cụ phân tích mã tự động để tìm và khắc phục các điểm có khả năng xảy ra lỗi tràn bộ đệm, đặc biệt lưu ý đến các hàm xử lý xâu ký tự.

Sử dụng cơ chế không cho phép thực hiện mã trong dữ liệu DEP (Data Excution Prevention). Cơ chế DEP được hỗ trợ bởi hầu hết các hệ điều hành (từ Windows XP và các hệ điều hành họ Linux, Unix,…) không cho phép thực hiện mã chương trình chứa trong vùng nhớ dành cho dữ liệu. Như vậy, nếu kẻ tấn công khai thác lỗi tràn bộ đệm, chèn được mã độc vào bộ đệm trong ngăn xếp, mã độc cũng không thể thực hiện.

Ngẫu nhiên hóa sơ đồ địa chỉ cấp phát các ô nhớ trong ngăn xếp khi thực hiện chương trình, nhằm gây khó khăn cho việc gỡ rối và phát hiện vị trí các ô nhớ quan trọng như ô nhớ chứa địa chỉ trở về.

Sử dụng các cơ chế bảo vệ ngăn xếp, theo đó thêm một số ngẫu nhiên (canary) phía trước địa chỉ trở về và kiểm tra số ngẫu nhiên này trước khi trở về chương trình gọi để xác định khả năng bị thay đổi địa chỉ trở về.

Sử dụng các ngôn ngữ, thư viện và công cụ lập trình an toàn. Trong các trường hợp có thể, sử dụng các ngôn ngữ không gây tràn, như Java, các ngôn ngữ lập trình trên nền Microsoft .Net. Với các ngôn ngữ có thể gây tràn như C, C++, nên sử dụng các thư viện an toàn (Safe C/C++ Libraries) để thay thế các thư viện chuẩn có thể gây tràn.

2.2. Lỗi không kiểm tra đầu vào

Lỗi không kiểm tra đầu vào (Unvalidated input) là một trong các dạng lỗ hổng bảo mật phổ biến, trong đó ứng dụng không kiểm tra, hoặc kiểm tra không đầy đủ các dữ liệu đầu vào, nhờ đó tin tặc có thể khai thác lỗi để tấn công ứng dụng và hệ thống. Dữ liệu đầu vào (Input data) cho ứng dụng rất đa dạng, có thể đến từ nhiều nguồn với nhiều định dạng khác nhau.

Các dạng dữ liệu đầu vào điển hình cho ứng dụng:

Các trường dữ liệu văn bản (text);

Các lệnh được truyền qua địa chỉ URL để kích hoạt chương trình;

Các file âm thanh, hình ảnh, hoặc đồ họa do người dùng, hoặc các tiến trình khác cung cấp;

Các đối số đầu vào trong dòng lệnh;

Các dữ liệu từ mạng hoặc từ các nguồn không tin cậy.

Phòng chống

Biện pháp chủ yếu phòng chống tấn công khai thác lỗi không kiểm tra đầu vào là lọc dữ liệu đầu vào. Tất cả các dữ liệu đầu vào, đặc biệt dữ liệu nhập từ người dùng và từ các nguồn không tin cậy cần được kiểm tra kỹ lưỡng. Các biện pháp cụ thể bao gồm:

Kiểm tra kích thước và định dạng dữ liệu đầu vào;

Kiểm tra sự hợp lý của nội dung dữ liệu;

Tạo các bộ lọc để lọc bỏ các ký tự đặc biệt và các từ khóa của các ngôn ngữ trong các trường hợp cần thiết mà kẻ tấn công có thể sử dụng:

+ Các ký tự đặc biệt: *, ‘, =, --

+ Các từ khóa ngôn ngữ: SELECT, INSERT, UPDATE, DELETE, DROP,.... (với dạng tấn công chèn mã SQL).

2.3. Các vấn đề với điều khiển truy nhập

Điều khiển truy nhập (Access control) là một lớp bảo vệ đặc biệt quan trọng trong hệ thống

các lớp bảo vệ hệ thống và dữ liệu. Điều khiển truy nhập liên quan đến việc điều khiển ai (chủ thể) được truy cập đến cái gì (đối tượng). Điều khiển truy nhập có thể được thiết lập bởi hệ điều hành, hoặc mỗi ứng dụng, và thường gồm 2 khâu: xác thực (Authentication) và trao quyền (Authorization).

Để đảm bảo an toàn cho hệ thống điều khiển truy nhập, các biện pháp sau cần được xem xét áp dụng:

- Không dùng tài khoản quản trị (root hoặc admin) để chạy các chương trình ứng dụng.
- Luôn chạy các chương trình ứng dụng với quyền tối thiểu, vừa đủ để chúng thực thi các tác vụ.
- Kiểm soát chặt chẽ người dùng, xóa bỏ hoặc cấm truy nhập với những người dùng ngầm định kiểu everyone.
- Thực thi chính sách mật khẩu an toàn.
- Chỉ cấp quyền vừa đủ cho người dùng thực thi nhiệm vụ.

2.4. Các điểm yếu trong xác thực, trao quyền

Do các khâu xác thực và trao quyền là hai thành phần cốt lõi của một hệ thống điều khiển truy nhập, nên các điểm yếu trong xác thực và trao quyền ảnh hưởng trực tiếp đến độ an toàn của hệ thống điều khiển truy nhập. Một điểm yếu điển hình trong khâu xác thực là mật khẩu được lưu dưới dạng rõ (plaintext), dẫn đến nguy cơ bị lộ mật khẩu rất cao trong quá trình truyền thông tin xác thực. Ngoài ra, việc sử dụng mật khẩu đơn giản, dễ đoán, hoặc dùng mật khẩu trong thời gian dài cũng là điểm yếu dễ bị khai thác. Việc sử dụng cơ chế xác thực không đủ mạnh, như các cơ chế xác thực đơn giản của giao thức HTTP cũng tiềm ẩn các nguy cơ bị tấn công khai thác.

Trong khâu trao quyền cũng tồn tại một số điểm yếu, như sử dụng cơ chế thực hiện trao quyền không đủ mạnh, dễ bị vượt qua. Chẳng hạn, một trang web chỉ thực hiện ẩn các links đến các trang web mà người dùng không được truy nhập mà không thực sự kiểm tra quyền truy nhập trên từng trang, nếu người dùng tự gõ URL của trang thì vẫn có thể truy nhập.

2.5. Các điểm yếu trong các hệ mật mã

Các vấn đề với các hệ mật mã bao gồm việc sử dụng giải thuật mã hóa, giải mã, hàm băm yếu, lạc hậu, hoặc có lỗ hổng đã biết không thể khắc phục (DES, MD4, MD5,...); Việc sử dụng khóa (key) mã hóa, giải mã yếu, như các khóa có chiều dài ngắn, hoặc dễ đoán. Các hệ mã hóa khóa bí mật có độ an toàn cao, tốc độ cao, nhưng gặp phải khó khăn trong vấn đề trao đổi, chia sẻ các khóa bí mật. Các khóa bí mật trao đổi trong môi trường không an toàn như mạng Internet có thể bị lộ, bị đánh cắp. Một số vấn đề khác có thể gặp phải với các hệ mã hóa, gồm các vấn đề xác thực người gửi, người nhận, vấn đề sử dụng các khóa, các chứng chỉ hết hạn hoặc bị thu hồi, hoặc chi phí tính toán lớn, đặc biệt đối với các hệ mã hóa khóa công khai.

2.6. Các lỗ hổng bảo mật khác

Các thao tác không an toàn với các file cũng có thể là một lỗ hổng bảo mật nghiêm trọng. Chẳng hạn, một người dùng thực hiện đọc/ghi file lưu ở những nơi mà những người dùng khác cũng có thể ghi file đó. Các lỗi điển hình khác có thể gồm:

Không kiểm tra chính xác loại file, định danh thiết bị, các links hoặc các thuộc tính khác của file trước khi sử dụng.

Cho phép tải file tài liệu, hình ảnh lên máy chủ nhưng không kiểm tra định dạng file và không cấm quyền thực hiện, và do vậy tin tặc có thể tải lên và thực hiện các file chứa mã độc;

Không kiểm tra mã trả về sau mỗi thao tác với file;

Giả thiết một file có đường dẫn cục bộ là file cục bộ và bỏ qua các thủ tục kiểm tra. Tin tặc có thể khai thác lỗi này bằng cách ánh xạ file ở xa vào hệ thống file cục bộ, tức là có đường dẫn cục bộ và có thể được thực thi trên hệ thống cục bộ.

Một dạng điểm yếu bảo mật khác xảy ra khi xuất hiện các điều kiện đua tranh (Race conditions). Một điều kiện đua tranh tồn tại khi có sự thay đổi trật tự của 2 hay một số sự kiện gây ra sự thay đổi hành vi của hệ thống. Đây là một dạng lỗi nếu chương trình chỉ có thể thực hiện đúng chức năng nếu các sự kiện phải xảy ra theo đúng trật tự. Tin tặc có thể lợi dụng khoảng thời gian giữa 2 sự kiện để chèn mã độc, đổi tên file hoặc can thiệp vào quá trình hoạt động bình thường của hệ thống.

III. KẾT LUẬN

Hệ điều hành và phần mềm ứng dụng đóng vai trò quan trọng trong việc vận hành các thiết bị và hệ thống công nghệ thông tin tại các cơ sở giáo dục. Tuy nhiên, trong quá trình sử dụng, các hệ

thống này vẫn tiềm ẩn nhiều dạng lỗ hổng khác nhau, xuất phát từ thiết kế, lập trình, cấu hình và cách thức khai thác, sử dụng. Các lỗ hổng này không chỉ ảnh hưởng đến tính ổn định của hệ thống mà còn tiềm ẩn nguy cơ mất an toàn thông tin, gián đoạn hoạt động dạy học và quản lý nhà trường.

Bài viết đã khái quát và phân tích một số dạng lỗ hổng thường gặp trong hệ điều hành và phần mềm ứng dụng, đồng thời chỉ ra những tác động của các lỗ hổng này đối với việc quản lý, khai thác và sử dụng thiết bị giáo dục. Qua đó cho thấy, việc nhận diện và hiểu rõ các dạng lỗ hổng là cơ sở quan trọng giúp các cơ sở giáo dục chủ động hơn trong công tác phòng ngừa rủi ro và bảo đảm an toàn cho hệ thống thiết bị công nghệ thông tin.

Từ góc độ thực tiễn, kết quả nghiên cứu của bài viết góp phần nâng cao nhận thức về an toàn thông tin cho đội ngũ cán bộ quản lý, giáo viên và nhân viên kỹ thuật trong nhà trường. Trên cơ sở đó, các cơ sở giáo dục có thể tăng cường công tác quản lý, lựa chọn và sử dụng hệ điều hành, phần mềm ứng dụng phù hợp, đồng thời chú trọng công tác bảo trì, cập nhật và khai thác thiết bị giáo dục một cách hiệu quả, an toàn và bền vững.

TÀI LIỆU THAM KHẢO

Phan Đình Diệu, (2004), *Lý thuyết mật mã và an toàn thông tin,* NXB Đại học Quốc gia Hà Nội.

Lê Quang Minh, (2015), *Bài giảng Nhập môn an toàn thông tin,* Đại học Quốc gia Hà Nội.

TS.Nguyễn Khang Văn, (2014)*, Cơ sở an toàn thông tin*, Đại học Bách Khoa Hà Nội.

Trịnh Nhật Tiến, (2007), *Bài giảng An ninh dữ liệu,* NXB Đại học Quốc gia Hà Nội.