

Hơn 95.000 máy chủ của Adobe Magento bị tấn công, doanh nghiệp Việt Nam cần khẩn trương ứng phó

18:11 03/11/2025

Các chuyên gia an ninh mạng Bkav đánh giá, Việt Nam nằm trong nhóm quốc gia có nguy cơ cao bị tấn công bởi lỗ hổng nghiêm trọng có tên gọi Session Reaper trên nền tảng thương mại điện tử của Adobe.



Hơn 95.000 máy chủ Magento (Adobe Commerce) trên toàn cầu đang bị tấn công bởi một lỗ hổng nghiêm trọng có tên gọi Session Reaper. Lỗ hổng này cho phép tin tặc lợi dụng phiên đăng nhập của người dùng để thực thi mã từ xa và kiểm soát toàn bộ hệ thống.

Các chuyên gia an ninh mạng Bkav đánh giá, Việt Nam nằm trong nhóm quốc gia có nguy cơ cao bị tấn công bởi lỗ hổng này.

Magento là một hệ thống quản lý nội dung thương mại điện tử (E-commerce CMS) mã nguồn mở, được phát triển bởi công ty Magento Inc. Magento được phát hành lần đầu vào năm 2008 và hiện nay đã trở thành một trong những nền tảng thương mại điện tử phổ biến nhất trên thế giới, được sử dụng bởi hàng

ngành các doanh nghiệp và cửa hàng trực tuyến lớn.

Ông Hoàng Trường Khương, chuyên gia an ninh mạng của Bkav, cho biết lỗ hổng SessionReaper xuất phát từ cách Magento xử lý dữ liệu thông qua Web API, cho phép kẻ tấn công chen nội dung độc hại vào phiên làm việc (session) và tải lên web shell - tệp mã độc giúp duy trì quyền truy cập và điều khiển máy chủ.

Khai thác thành công, tin tặc có thể chiếm quyền quản trị hệ thống, rò rỉ dữ liệu thanh toán hoặc tạo tài khoản quản trị giả để mở rộng phạm vi tấn công. Các phiên bản Adobe Commerce và Magento Open Source phát hành trước tháng 10/2025, bao gồm các nhánh từ 2.4.9-alpha2 trở xuống đều dính lỗ hổng này.

Chỉ trong 48 giờ sau khi mã khai thác công khai, thế giới đã ghi nhận hơn 300 cuộc tấn công tự động nhắm vào hơn 130 máy chủ Magento. Theo thống kê của Sansec Shield, dù Adobe đã phát hành bản vá khẩn cấp từ đầu tháng 9, đến nay vẫn còn khoảng 62% cửa hàng Magento chưa được cập nhật.

Với hơn 95.000 máy chủ Magento đang hoạt động công khai trên toàn cầu, con số này đồng nghĩa hàng nghìn website thương mại điện tử vẫn đang trong tình trạng dễ bị tấn công. Việc chậm trễ cập nhật chỉ một ngày cũng có thể khiến doanh nghiệp chịu thiệt hại nặng nề.

Tại Việt Nam, rất nhiều sàn thương mại điện tử, trong đó phải kể đến hàng trăm thương hiệu nổi tiếng trong lĩnh vực bán lẻ, thời trang và công nghệ... đang sử dụng Magento. Các nghiên cứu, khảo sát cũng như kinh nghiệm từ quá trình xử lý sự cố an ninh mạng của Bkav, đều cho thấy đây là nhóm mục tiêu dễ bị tổn thương nhất vì hầu hết hệ thống không có quy trình vá lỗi định kỳ hoặc thiếu lớp phòng thủ ở tầng ứng dụng (WAF).

Trong khi đó, các phiên bản Magento cũ hoặc module REST API chưa được kiểm soát được đánh giá là nhóm rủi ro cao, có khả năng bị tin tặc khai thác nhanh nếu không cập nhật kịp thời.

Bkav khuyến nghị các quản trị viên hệ thống Magento tại Việt Nam cần khẩn trương cập nhật bản vá chính thức từ Adobe, đồng thời kích hoạt tường lửa ứng dụng web (WAF) để lọc và chặn các gói tin bất thường. Các doanh nghiệp nên rà soát toàn bộ hệ thống, đặc biệt là kiểm tra sự xuất hiện của tệp PHP lạ trong thư mục, xem lại các tài khoản quản trị mới phát sinh. Trường hợp nghi ngờ bị xâm nhập, cần cách ly máy chủ, khôi phục từ bản sao lưu sạch và thay đổi toàn bộ mật khẩu, khóa truy cập.

Theo nhandan.vn