CISCO LẠI PHẢI VÁ LỖI BẢO MẬT SẢN PHẨM

Cisco vừa cho khắc phục một số lỗi bảo mật trong ứng dụng CS-MARS (Cisco Security Monitoring, Analysis and Response System). Theo nhà phát triển, những lỗi bảo mật này có thể bị tin tặc khai thác từ xa để đoạt quyền truy cập bất hợp pháp tới các thiết bị nhạy cảm. Ứng dụng CS-MARS kiểm tra giá

Cisco vừa cho khắc phục một số lỗi bảo mật trong ứng dụng CS-MARS (Cisco Security Monitoring, Analysis and Response System). Theo nhà phát triển, những lỗi bảo mật này có thể bị tin tặc khai thác từ xa để đoạt quyền truy cập bất hợp pháp tới các thiết bị nhạy cảm. Ứng dụng CS-MARS kiểm tra giám sát các vấ đề bảo mật trên các thiết bị mạng bằng cách kiểm tra cấu hình các bộ định tuyến (routers) và bộ chuyển mạch (switches). Đồng thời ứng dụng này còn cho phép các doanh nghiệp có thể kiểm tra mức độ bảo mật hệ thống hạ tầng cơ sở mạng của mình bằng cách đối chiếu với danh sách các lỗi bảo mật đã được phát hiện. Được biết lỗi bảo mật mới được Cisco cho vá chỉ ảnh hưởng đến các phiên bản CS-MARS từ 4.2.1 hoặc cũ hơn. Cisco đã phát hành bản vá để khắc phục lỗi bảo mật nói trên. Người dùng có thể tải về thông qua trang web của hãng. Nguyên nhân Ứng dụng máy chủ web JBoss trong CS-MARS chính là nguyên nhân sinh ra lỗi bảo mật nói trên. Tin tặc có thể lợi dụng ứng dụng này để từ xa đăng nhập và gửi các yêu cầu HTTP tới ứng dụng CS-MARS cho phép chúng có thể thực hiện các mã lệnh với quyền ưu tiên cấp quản trị. Ngày hôm qua (19/7), chuyên gia nghiên cứu bảo mật Jon Hart đã công bố đoạn mã được chứng minh là có đầy đủ khả năng khai thác lỗi JBoss thông qua Full-Disclosure. Trong bài viết của mình, chuyên gia bảo mật này cho biết JBoss phiên bản 3.2.7 mắc lỗi bảo mật trong giao diện điều khiển JMX Console khiên tin tặc có thể xem được thông tin nhân vi mô (microkernel) của ứng dụng máy chủ JBoss. Trong khi đó, một lỗi bảo mật khác trong cơ sở dữ liệu Oracle đi kèm với CS-MARS và có thể được sử dụng để lưu trữ các thông tin về mạng cũng như các thông tin chứng thực đăng nhập tường lửng, routers hoặc thiết bị IPS. Tuy nhiên, cơ sở dữ liệu Oracle lại chứa một số tài khoản đăng nhập mặc định với những mật khẩu (password) mà ai cũng biết? Chính vì thế mà tin tặc có thể dễ dàng lấy đi những thông tin trong cơ sở dữ liệu giúp chúng tấn công thiết bị mạng. Tuy nhiên, ứng dụng CS-MARS lại không sử dụng các tài khoản mặc định cơ sở dữ liệu Oracle và đã được khắc phục lỗi bảo mật trên nhằm tránh những truy cập trái phép đến cơ sở dữ liệu. Những tài khoản đó đã bị vô hiệu hoá. Bên cạnh đó, một số lỗi bảo mật khác trong Giao diện điều khiển dòng lệnh CS-MARS cũng có thể cho phép người quản trị thực thi các đoạn mã nhị phân với quyền ưu tiên gốc (root level). Tuy nhiên, hãng bảo mật Symantec không đánh giá cao những lỗi bảo mật nói trên. Symantec chỉ xếp những lỗi đó vào cấp độ 10 trên chiếc thang 10 bậc đánh giá mức độ nguy hiểm các lỗi bảo mật. Hoàng Dũng