CISCO CALL MANAGER MỞ CỬA ĐÓN CHÀO TIN TẶC

Các lỗ hổng bảo mật trong phần mềm Cisco Call Manager có thể tạo cơ hội cho tin tặc cấu hình lại thiết lập VoIP và đoạt quyền truy cập vào thông tin tài khoản cá nhân người sử dụng. Đây là những gì mà các chuyên gia của nhà cung cấp giải ph&a

Các lỗ hổng bảo mật trong phần mềm Cisco Call Manager có thể tạo cơ hội cho tin tặc cấu hình lại thiết lập VoIP và đoạt quyền truy cập vào thông tin tài khoản cá nhân người sử dụng. Đây là những gì mà các chuyên gia của nhà cung cấp giải pháp FishNet Security cảnh báo người dùng trong một bản báo cáo phát hành hôm 19/6. Jake Reynolds - chuyên gia bảo mật cao cấp của FishNet - cho biết phần mềm Call Manager từ phiên bản 3.1 trở lên đều mắc những lỗi bảo mật này. Lỗi bảo mật này phát xinh trong chức năng định tuyến và phát tin hiệu cuộc gọi trong các hệ thống VoIP của Cisco. Reynolds khẳng định do thiếu khả năng kiểm soát chứng thực đầu vào và đầu ra được lập trình đưa lên giao diện quản lý web cho Call Manager nên tin tặc mới có thể lợi dụng để từ xa thực thi các vụ tấn công cross-site scripting. Kiểu tấn công cross-site scripting thường được sử dụng để lừa người sử dụng có quyền ưu tiên truy cập nhắp chuột vào một đường siêu liên kết URL chứa trong một email hoặc một trang web. Trong trường hợp của Call Manger, tin tặc sẽ gửi một yêu cầu có chứa các đoạn mã JavaScript độc hại tới giao diện quản trị web Call Manager. Nếu người quản trị bị lừa và chấp nhận yêu cầu này, đoạn mã độc hại có thể sẽ được thực thị trên trình duyệt web của họ và cho phép kẻ tấn công có quyền xoá hoặc tái cầu hình lại các thành phần hệ thống hoặc đoạt quyền truy cập tới các thông tin tài khoản bí mật của người dùng. Trong một bài phát biển, Cisco Product Security Incident Response Team (PSRIT) khuyến cáo người sử dụng nên xác nhận điểm đến các đường liên kết trước khi nhắp chuột vào. Cisco đã khắc phục các lỗi bảo mật này và sẽ tích hợp các bản vá vào trong các phiên bản Call Manager 4.3(1), 4.2(3), 4.1(3)SR4 và 3.3(5) SR3. Hoàng Dũng