THÊM MỘT LỖI BẢO MẬT TRONG SẢN PHẨM CISCO

Một lỗ hổng bảo mật nằm trong Cisco Secure Access Control Server (ACS) vừa mới được phát hiện và công bố. Cisco Secure Access Control Server (ACS) là một bộ phận quan trọng trong khung quản lý tin cậy và nhận dạng của Cisco. Đây cũng là một trong những nền tảng của sáng kiến Cisco Network

Một lỗ hổng bảo mật nằm trong Cisco Secure Access Control Server (ACS) vừa mới được phát hiện và công bố. Cisco Secure Access Control Server (ACS) là một bộ phận quan trọng trong khung quản lý tin cậy và nhận dạng của Cisco. Đây cũng là một trong những nền tảng của sáng kiến Cisco Network Admission Control (NAC). Secure ACS là một giải pháp mạng lưới nhận dạng giúp đơn giản hoá việc quản lý người dùng bằng cách kết hợp cấp quyền truy cập chứng thực, người dùng, nhà quản trị với chính sách quản lý. Lỗ hổng bảo mật phát sinh trong Secure ACS có thể cho phép tin tặc đoạt quyền truy cập cấp quản trị vào giao diện dạng web phần mềm quản lý thiết bị mạng. Darren Bounds - một chuyên gia nghiên cứu bảo mật độc lập - là người đã phát hiện và tiết lộ thông tin về lỗi bảo mật này thông qua danh sách email bảo mật Full Disclosure. Secure ACS là một đấu mối quan trọng trong hệ thống khung Cisco NAC. Secure ÁC chủ yếu dựa trên khả năng của người dùng và thiết bị đầu cuối để chứng thực quyền truy cập vào các thư mục trung tâm. "Không may là nếu khai thác thành công lỗi bảo mật trong Secure ACS kẻ tấn công có thể đoạt được quyền truy cập cấp quản trị tới bất kỳ một thiết bị nào mà máy chủ ACS nắm giữa quyền chứng thực truy cập," Bounds nói. Lỗi bảo mật này là khá dễ khai thác vì những thông tin cần thiết để khai thác có thể dễ dàng thu thập được hoặc đã tồn tại sẵn trong một số trường hợp. Lấy ví dụ, rất nhiều công ty xử lý việc cấp quyền truy cập Secure ACS thông qua một proxy - hay đồng nghĩa với việc tất cả các máy khách đều có chung một địa chỉ IP. Để khai thác lỗi bảo mật này, kẻ tấn công cần tìm ra một cổng động được máy chủ ACS quản lý. Thông tin này rất dễ tìm do hầu hết hiện nay các Secure ACS đều sử dụng việc cấp cổng tự động. "Rất dễ dự đoán xem nhà quản trị có đăng nhập hay không để tìm xem cổng nào mà họ đang sử dụng. Và vì chỉ có khoảng 65.000 cổng kết hợp được sử dụng, kẻ tấn công có thể chỉ cần chạy qua mọi cổng là đã phát hiện được cổng mà hắn cần," Bounds cho biết thêm. Ngày hôm qua, Cisco Product Security Incident Response Team (PSRIT) cho biết họ đang điều tra thêm về lỗ hổng bảo mật này. Hoàng Dũng