CISCO CẢNH BÁO 2 LỖI BẢO MẬT NGHIÊM TRỌNG

Cisco

Cisco Systems vừa phát hành bản tin cảnh báo người dùng về hai lỗi bảo mật nghiêm trọng trong thiết bị điều khiển mạng Cisco NAC Appliance.

Thông tin từ phía nhà sản xuất cho biết hai lỗi bảo mật này có thể bị tin tặc lợi dụng để chiếm quyền kiểm soát thiết bị mắc lỗi hoặc ăn cắp các thông tin nhạy cảm như mật khẩu đăng nhập...

Cisco NAC Appliance - hay còn được biết đến với tên gọi Cisco Clean Access (CCA) - là thiết bị đảm trách nhiệm vụ xác nhận thiết bị ngoại vi có yêu cầu kết nối vào hệ thống mạng của doanh nghiệp đáp ứng đủ các yêu cầu chính sách bảo mật.

Lỗi thứ nhất

Lỗi bảo mật thứ nhất được đặt tên là "Unchangeable Shared Secret". Lỗi này bắt nguồn từ việc dữ liệu Shared Secret không được thiết lập hoặc thay đổi đúng cách trong khi cài đặt thiết bị. Hay nói một cách khác dữ liệu Shared Secret là giống nhau trên mọi thiết bị.

Shared Secret là dữ liệu cho phép cho phép Clean Access Manager (CAM) gửi chứng thực xác nhận thiết bị tới Clean Access Server (CAS).

Để khai thác thành công lỗi "Unchangeable Shared Secret" tin tặc phải thiết lập được một kết nối TCP tới CAS. Nếu thành công thì tin tặc sẽ giành được quyền kiểm soát ở cấp độ người quản trị tới một CAS bất kỳ.

Các phiên bản CCA mắc lỗi "Unchangeable Shared Secret" gồm phiên bản 3.6.x đến 3.6.4.2 và phiên bản 4.0.x đến 4.0.3.2.

Người dùng được khuyến cáo là nên nâng cấp lên phiên bản 3.6.4.3, 4.0.4 và 4.1.0 hoặc truy cập vào trang web của Cisco để tải về bản vá lỗi có tên Patch-CSCsg24153.tar.gz. Lưu ý chỉ có những khách hàng đã ký kết Cisco Service Agreement mới có thể truy cập vào tải về các bản vá lỗi.

Lỗi thứ hai

Lỗi bảo mật thứ hai được đặt tên là "Readable Snapshots". Với lỗi này, tin tặc hoàn toàn có thể sử dụng biện pháp tấn công brute-force để tải về cơ sở dữ liệu backup - hay còn gọi là các snapshot - trên CAM mà không cần phải được cấp quyền. Trong khi đó, những tệp tin backup đó lại không hề được mã hoá hoặc bảo vệ bằng bất kỳ một giải pháp nào.

Nguy hiểm hơn những tệp tin snapshot đó lại chứa những thông tin có thể trợ giúp cho tin tặc trong việc tấn công CAS hoặc được dùng để chiếm quyền điều khiển CAM.

Các phiên bản mắc lỗi gồm CCA phiên bản 3.5.x đến 3.5.9 và phiên bản 3.6.x đến 3.6.1.1. Người dùng được khuyến cáo là nên nâng cấp lên phiên bản 3.5.10 và 3.6.2.

Hiện Cisco chưa phát hành bản cập nhật vá lỗi snapshot. Tuy nhiên, nhà sản xuất khuyến cáo người dùng nên di chuyển các tệp tin snapshot ra khỏi thiết bị ngay sau khi tiến hành backup dữ liệu.

Nhóm phản ứng nhanh với các tình huống bảo mật của Cisco khẳng định đến thời điểm này vẫn chưa hề xuất hiện bất kỳ một mã khai thác lỗi nào có thể tấn công hai lỗi trên được phát tán lên Internet.

Hoàng Dũng