CISCO BÍT LỖ HỔNG TRÌNH ĐIỀU KHIỂN THIẾT BỊ MẠNG

Ngày hôm qua (02/11), Cisco Systems vừa mới cho bít một lỗ hổng bảo mật quan trọng trong phần mềm điều khiển bộ định hướng (router) và thiết bị chuyển mạch mạng (switch). Lần này, hãng sản xuất thiết bị mạng hàng đầu thế giới đã cho ban hành một bản cập nhật nhằm vá lỗ hổng tr&agr

Ngày hôm qua (02/11), Cisco Systems vừa mới cho bít một lỗ hổng bảo mật quan trọng trong phần mềm điều khiển bộ định hướng (router) và thiết bị chuyển mạch mạng (switch). Lần này, hãng sản xuất thiết bị mạng hàng đầu thế giới đã cho ban hành một bản cập nhật nhằm vá lỗ hổng tràn bộ nhớ đệm trong phần mềm điều khiển thiết bị mạng Internetwork Operating System - một lỗi bảo mật thường thấy trong các phần mềm. Tuy nhiên, lỗi này cũng rất nguy hiểm vì nó cho phép kẻ tấn công từ xa đoạt được quyền kiểm soát hệ thống bị mắc lỗi. Trong trường hợp này là giành được quyền kiểm soát điều khiển các bộ định hướng và thiết bị chuyển mạch mạng của Cisco - những thiết bị cơ sở hạ tầng của cả một hệ thống mạng máy tính bao gồm cả mạng Internet. Trên thực tế lỗi bảo mật trong IOS được vá lần này đã được công bố tại diễn đàn bảo mật Black Hat tháng 7 vừa qua. Nhưng Cisco đã giữ bí mật cho đến tận ngày hôm nay. Tại diễn đàn Black Hat, chuyên gia nghiên cứu bảo mật Michael Lynn đã chứng minh khả năng đoạt quyền điều khiển kiểm soát các bộ định hướng (router) bằng cách khai thác lỗi bảo mật trong phần mềm điều khiển. Và nếu lỗi bảo mật này được khai thác phục vụ cho một cuộc tấn công quy mô rộng thì hậu quả sẽ khôn lường – có thể khiến cho mạng máy tính Internet hay của một doanh nghiệp ngừng hoạt động. John Noh, người phát ngôn của Cisco, cho biết: "Lynn đã lợi dụng lỗ hổng bảo mật trong IPv6 đã được cho công bố hồi tháng 7 vừa qua để tiến hành một cuộc tấn công tràn bộ nhớ đệm lên bộ đếm giờ hệ thống. Lỗi này Cisco đã cho vá từ hồi tháng 4 nhưng Lynn vẫn có thể lợi dụng để tấn công và điều khiển các router." Sự thật là trong tháng 7 Cisco đã cho công bố chi tiết lỗ hổng bảo mật trong IPv6 - lỗi mà Lynn đã sử dụng để làm ví dụ chứng minh tại diễn đàn Black Hat. Nhưng vẫn còn một lỗi khác nguy hiểm hơn mà nhà phát triển lại không cho công bố. Phải đến ngày hôm qua thì người sử dụng mới biết đến lỗi này. Có thể thấy rằng phạm vi ảnh hưởng của lỗi bảo mật này quá lớn nên buộc Cisco phải giữ im lặng, Johannes Ullrich, chuyên gia nghiên cứu trưởng của Viện nghiên cứu SANS bày tỏ quan điểm. "Tính chất nguy hiểm của những lỗi bảo mật này là câu trả lời tại sao Cisco phải giữ bí mật không cho công bố tại diễn dần Black Hat. Nếu như chúng ta ai cũng biết về lỗi bảo mật này thì có thể hậu quả sẽ khó lường". Ullrich khuyến cáo người sử dụng tiến hành cập nhật trình điều khiển thiết bị càng sớm càng tốt. Bên cạnh việc vá lỗ hổng bảo mật tràn bộ nhớ đệm, Cisco cũng cho tăng cường khiên chắn bảo mật cho phần mềm này. Phiên bản phần mềm mới được bổ sung thêm nhiều tính năng kiểm tra tính toàn vẹn (integrity check) nhằm phát hiện và phòng tránh các cuộc tấn công trong tương lai. Cisco cho rằng sau khi hãng cho công bố chi tiết về lỗi bảo mật này thì hãng cũng không lo sợ rằng lỗi này có thể bị lợi dụng để tổ chức các cuộc tấn công. Bản cập nhật cho mọi phiên bản IOS hiện đã có thể tải về trên trang web của nhà sản xuất. HVD - (CNet)