CISCO BÍT 3 LỖ HỔNG NGUY HIỂM TRONG IOS

Cisco vừa phát hành bản cập nhật để bít 3 lỗi hổng bảo mật phát sinh trong IOS - hệ điều hành điều khiển thiết bị mạng switch và router.

Theo bản tin cảnh báo của Cisco, lỗi bảo mật nguy hiểm nhất trong số những lỗi được khắc phục đợt này là lỗi tràn bộ nhớ đệm và cho

Cisco vừa phát hành bản cập nhật để bít 3 lỗi hổng bảo mật phát sinh trong IOS - hệ điều hành điều khiển thiết bị mạng switch và router.

Theo bản tin cảnh báo của Cisco, lỗi bảo mật nguy hiểm nhất trong số những lỗi được khắc phục đợt này là lỗi tràn bộ nhớ đệm và cho phép tin tặc có thể thực thi các mã độc trên thiết bị mắc lỗi.

Tin tặc có thể khai thác lỗi này bằng cách gửi đi các gói tin được lập trình đặc biệt thông qua thủ tục Internet Control Message Protocol (ICMP), Protocol Independent Multicast version 2 (PIMv2), Pragmatic General Multicast (PGM) hoặc URL Rendezvous Directory (URD) tới thiết bị mắc lỗi.

Mọi thiết bị chạy phiên bản Cisco IOS hoặc Cisco IOS XR đều mắc những lỗi bảo mật trên. Tuy nhiên, chỉ những thiết bị được cấu hình cho phép xử lý gói tin IPv4 là có thể bị tấn công.

Những thiết bị chạy IPv6 hoàn toàn vô hại. Nhưng những thiết bị này lại mắc phải mỗi lỗi bảo mật khác có thể bị tin tặc lợi dụng để làm cho router ngừng hoạt động liên tục, gây ra tình huống từ chối dịch vụ. Đây cũng chính là điều kiện cần thiết giúp tin tặc có thể từ xa thực thi các mã độc trên thiết bị.

Chris Labatt-Simon - Chủ tịch kiêm giám đốc điều hành của nhà cung cấp giải pháp mạng D&D Consulting - đánh giá lỗi IPv6 mới thực sự là lỗi nguy hiểm bởi nó tồn tại trên hầu hết mọi phiên bản IOS và rất dễ bị khai thác.

Lỗi bảo mật thứ 3 được khắc phục trong đợt này là lỗi nằm trong bộ phận nhận tín hiệu TCP trên một số phiên bản IOS. Lỗi này có thể bị tin tặc lợi dụng để tổ chức các vụ tấn công từ chối dịch vụ lên thiết bị.

Khách hàng được khuyến cáo là nên nhanh chóng tải về và cài đặt các bản vá lỗi sớm chừng nào tốt chừng đó.

Hoàng Dũng