CISCO CHƯA TÌM THẤY LỖ HỔNG TRONG PIX

Sau hai tuần điều tra theo yêu cầu của một chuyên gia nghiên cứu bảo mật độc lập, Cisco vừa khẳng định không thể tìm thấy lỗ hổng trong dòng sản phẩm PIX 500 Series Security Appliances. Tại Hội nghị Black Hat mới được tổ chức đầu tháng vừa rồi, Hendrik Scholz, một nhà phát triển VoIP v&agra

Sau hai tuần điều tra theo yêu cầu của một chuyên gia nghiên cứu bảo mật độc lập, Cisco vừa khẳng định không thể tìm thấy lỗ hổng trong dòng sản phẩm PIX 500 Series Security Appliances. Tại Hội nghị Black Hat mới được tổ chức đầu tháng vừa rồi, Hendrik Scholz, một nhà phát triển VoIP và là kỹ sư hệ thống hàng đầu của công ty Freenet Cityline (Đức), đã tuyên bố phát hiện một lỗ hổng chưa được công bố trong dòng sản phẩm PIX 500. Lỗ hổng này liên quan tới cách thức các ứng dụng xử lý thông điệp Session Initiation Protocol (SIP). Hendrik Scholz đã không tiết lộ nhiều thông tin về lỗ hổng trên cũng như cách thức khai thác chúng. Scholz cam kết hợp tác với Cisco để giải quyết lỗ hổng mới. Tuy nhiên, trong thông báo ngày 15/8, Nhóm phản ứng bảo mật sản phẩm của Cisco (PSIRT) đã cho biết không thể xác định được lỗ hổng như thông báo của Hendrik Scholz. Cũng theo Cisco, Scholz cho rằng chỉ cần một thông điệp SIP đặc biệt gửi tới PIX là có thể tạo ra một kết nối User Datagram Protocol (UDP) mở đối với bất cứ thiết bị nào trong mạng liên kết, cho phép kẻ tấn công có thể gửi giao vận UDP tới thiết bị bên trong mạng. Cisco cũng không thể giả lập được tình huống lỗ hổng dựa trên mô tả của Scholz trình bày tại Hội nghị Black Hat. "Hiện chúng tôi vẫn tiếp tục hợp tác với ông Scholz để tìm hiểu về lỗ hổng trên", tuyên bố của Cisco cho biết.