SÂU "GÀ TÂY" TẤN CÔNG HỆ ĐIỀU HÀNH SOLARIS 10

Solari

Solaris 10 OS của Sun Microsystems đang bị một loại sâu mới mệnh danh là "gà tây" tấn công từ cuối tháng trước nhờ lợi dụng lỗ hổng có trong hệ điều hành này.

Sâu mới có tên là Unix/Froot-A (hoặc Wanuk) và sở dĩ có tên "gà tây" là bởi trong phần mã nguồn của sâu này có hình con gà tây vẽ bằng các ký tự ASCII.

Lỗ hổng zero-day bị Unix/Froot-A khai thác đã được Sun vá lại sau 3 ngày kể từ khi những dòng mã khai thác đầu tiên được tung ra từ cuối tháng trước. Lỗ hổng nằm trong tiến trình Telnet, dùng để kết nối các client Telnet với nhau, có thể cho phép tin tặc truy cập vào hệ thống mà không cần tới mật khẩu. Kẻ tấn công có thể kiểm soát hoàn toàn hệ thống thông qua lỗ hổng này.

Unix/Froot-A quét cổng 23 để kiểm tra xem Telnet có chạy hay không, rồi sau đó gửi dữ liệu nhằm khai thác lỗ hổng. Những máy tính bị lây nhiễm sau đó sẽ thực hiện nhiệm vụ quét những máy tính khác để tìm kiếm lỗ hổng.

Hãng bảo mật Sophos cho biết hiện vẫn chưa nhận được báo cáo về trường hợp tấn công Sun Microsystems thông qua lỗ hổng trên. Người dùng Solaris được khuyến nghị cài đặt bản sửa lỗi mới nhất và vô hiệu hoá tính năng Telnet.