BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 26 tháng 9 năm 2014

Khẩn trương kiểm tra và khắc phục lỗ hổng an toàn thông tin CVE-2014-6271 trên hệ điều hành Linux, Unix

Ngày 24/9/2014, lỗ hổng an toàn thông tin rất nguy hiểm của hệ điều hành Linux và Unix đã được một số tổ chức quốc tế công bố và đặt mã số quốc tế là CVE-2014-6271 (theo tổ chức Mitre). Lỗ hổng này được đánh giá ở mức nghiêm trọng cao nhất, cho phép tin tặc có khả năng thực hiện một số lệnh điều khiển từ xa (Remote exploit vulnerability in bash) hoạt động hệ thống có lỗ hổng CVE-2014-6271 mà không cần tài khoản và mật khẩu đăng nhập.

Lỗ hổng CVE-2014-6271 nằm trong ứng dụng có tên là Bash Shell, ứng dụng này được cài đặt sẵn trong hầu hết các máy tính sử dụng hệ điều hành Linux và Unix. Do đó, phạm vi ảnh hưởng của lỗ hổng này sẽ bao gồm hầu hết các hệ thống máy trạm, máy chủ sử dụng hệ điều hành Linux, Unix và đồng thời có khả năng ảnh hưởng tới rất nhiều thiết bị nhúng (Embeded), thiết bị mạng (Router, Access point, Switch), các hệ thống thiết bị SCADA/ICS đang sử dụng hệ điều hành Linux.

Lỗ hổng trên có thể bị tin tặc khai thác từ xa thông qua một số dịch vụ trực tuyến trên máy tính có tồn tại lỗ hổng CVE-2014-6271, ví dụ một số dịch vụ cung cấp trực tuyến phổ biến này là:

- Dịch vụ Web của ứng dụng Apache,
- Dịch vụ điều khiển từ xa thông qua Telnet, SSH v.v… hoặc một số ứng dụng trực tuyến khác có cơ chế cho phép thực thi các lệnh của Bash Shell.

Qua khảo sát nhanh của Trung tâm VNCERT, tỷ lệ các máy chủ Linux cung cấp dịch vụ trực tuyến được kiểm tra có lỗ hổng an toàn thông tin CVE-2014-6271 là khá cao.

Phương pháp kiểm tra hệ thống bị ảnh hưởng bởi lỗ hổng CVE-2014-6271**:**

- Bước 1: Quản trị hệ thống truy cập vào Bash Shell của hệ thống cần kiểm tra.
- Bước 2: Thực hiện tuần tự hai câu lệnh sau đây từ bàn phím:

  env X="() { :;} ; echo Co_Diem_Yeu" /bin/sh -c "echo completed"

  env X="() { :;} ; echo Co_Diem_Yeu " `which bash` -c "echo completed"

Nếu chỉ một trong hai lệnh trên cho kết quả trên màn hình là "Co_Diem_Yeu" thì hệ thống đang kiểm tra có lỗ hổng CVE-2014-6271.

Các biện pháp cần ưu tiên thực hiện khi hệ thống có lỗi:

- Nâng cấp các bản vá lỗi hệ điều hành hoặc tắt phần mềm Bash Shell (sử dụng Korn Shell hoặc các phần mềm Shell khác để thay thế).
- Kiểm tra, rà soát nhật ký hoạt động, các thiết bị an toàn mạng để kịp thời phát hiện các hành vi xâm phạm hệ thống trái phép đã xảy ra để có biện pháp khắc phục kịp thời.
- Sử dụng tường lửa, thiết bị IPS hoặc các thiết bị bảo mật để hạn chế các tấn công và xâm nhập trái phép từ bên ngoài.
- Đặc biệt quan tâm các hệ thống trang thông tin điện tử, hệ thống cho phép điều khiển từ xa (SSH, Telnet v.v…) sử dụng hệ điều hành Linux.

Đề nghị Quý cơ quan, đơn vị nhanh chóng kiểm tra rà soát và khắc phục sớm lỗ hổng CVE-2014-6271 nêu trên. Nếu Quý cơ quan gặp sự cố này, đề nghị thông báo trực tiếp cho Trung tâm VNCERT để nắm tình hình số lượng, kết quả khắc phục nhanh và có biện pháp hỗ trợ nếu cần thiết. Mọi thông tin chi tiết xin liên hệ kỹ sư Trần Tuấn Anh, phòng Kỹ thuật hệ thống theo số điện thoại 043.3640.4424, hòm thư điện tử ttanh@vncert.vn.

Trân trọng./.