

Tuân thủ nguồn mở (*Open source Compliance*)- chìa khóa giảm thiểu nguy cơ bảo mật cho phần mềm thương mại

Nguyễn Hồng Quang – VFOSSA

Tóm tắt:

Open source có mặt ở mọi nơi. Các PM thương mại hầu như đều có chứa các thành phần open source và với tỷ trọng rất đáng kể, thậm chí là nền tảng. Tuy nhiên các báo cáo thường niên « Phân tích bảo mật nguồn mở và nguy cơ » (“Open Source Security and Risk Analysis” - OSSRA) của nhà kiểm toán phần mềm nổi tiếng Black Duck/Synopsys từ 7 năm qua đã chỉ ra rằng open source thường được sử dụng khá cẩu thả, không tuân thủ nguồn mở (*open source compliance*) trong các phần mềm thương mại. Và hệ lụy đi kèm với đó là phần mềm thương mại tiềm ẩn rất nhiều nguy cơ bảo mật. Bài trình bày này sẽ điểm lại một số báo cáo OSSRA những năm gần đây để chỉ ra xu hướng sử dụng các thành phần open source trong các PM thương mại đang diễn ra như thế nào và đang có những vấn đề gì về bảo mật cũng như nguy cơ của việc sử dụng open source không tuân thủ. Qua đó cảnh báo các nhà phát triển về tầm quan trọng của việc tuân thủ nguồn mở nhằm giảm thiểu nguy cơ bảo mật cho phần mềm.