BIẾN THỂ MỚI SÂU KHAI THÁC LỖI ORACLE

Đoạn mã độc hại có khả năng khai thác lỗ hổng bảo mật và gây thiệt hại nghiêm trọng cho phần mềm cơ sở dữ liệu Oracle phát tán trước đây đã được sửa đổi và tái phân phát rộng rãi trên Internet, rung lên một hồi chuông cảnh b&aacute

Đoạn mã độc hại có khả năng khai thác lỗ hổng bảo mật và gây thiệt hại nghiêm trọng cho phần mềm cơ sở dữ liệu Oracle phát tán trước đây đã được sửa đổi và tái phân phát rộng rãi trên Internet, rung lên một hồi chuông cảnh báo mới về một đợt tấn công mới. Như vậy, chỉ hai tháng sau kho một nhà nghiên cứu giấu tên lần đầu tiên cho công bố một ví dụ về sâu máy tính tấn công khai thác lỗ hổng bảo mật trong phần mềm cơ sở dữ liệu Oracle thì đoạn mã độc hại này đã được nghiên cứu cải tiến và tái phát tán thông qua danh sách thư điện tử Full Disclosure. Lại thêm một kĩ thuật mới để tấn công hệ cơ sở dữ liệu này. Tuy nhiên, Alexander Kornbrust – giám đốc điều hành của hãng bảo mật cơ sở dữ liệu GmbH, lại cho rằng: "Những phương thức tấn công kiểu như thế này hiện còn mang nặng tính lý thuyết và tôi không cho rằng các ứng dụng cơ sở dữ liệu lại có thể bị đe doạ vì những nguy cơ như thế này. Nếu như bạn đang phải quản trị một công ty lớn với hàng trăm cơ sở dữ liệu có giá trị thì đoạn mã này thực sự là một kẻ huỷ diệt. Đoạn mã độc hại này rất có thể sẽ được sử dụng để phát triển thành một loại sâu hoàn chỉnh. Cẩn thận có lẽ là điều nên làm nhất" Kornbrust - một chuyên gia rất nổi tiếng với những nghiên cứu bảo mật các sản phẩm của Oracle – cho rằng bản thân ông cũng đã tạo ra được một phương thức tấn công thực sự sử dụng tên đăng nhập và mật khẩu mặc định trong các cơ sở dữ liệu Oracle. Aaron Newman, kĩ sư công nghệ cao cấp tại Application Security Inc., mô tả đoạn mã mới này như là một cái gì đó "tiên tiến hơn rất nhiều" so với đoạn mã trước đây. "Tuy nhiên nó vẫn còn thiếu đi tính ứng dụng thực tế để có thể phát tán rộng rãi mặc dù bản thân chúng có khả năng như vậy." Kornbrust khuyến cáo các nhà quản trị cơ sở dữ liệu cần phải thận trọng trước nguy cơ bị tấn công dựa vào các lỗ hổng bảo mật trên máy tính trạm cộng với đoạn mã nguy hiểm khai thác lỗi bảo mật của Oracle. "Một vụ tấn công thành công có thể nhắm mục tiêu đến các ứng dụng cơ sở dữ liệu thông qua một lỗ hổng của Windows, đoạt quyền truy cập hệ thống các sử dụng sâu Oracle để gây ra những thiệt hại nghiêm trọng."