XUẤT HIỆN ĐOẠN MÃ NGUY HIỂM KHAI THÁC LỖI ORACLE

Một hacker giấu mặt vừa mới cho công một đoạn mã nguy hiểm nhằm khai thác lỗ hổng bảo mật gần đây.

Chủ tịch tập đoàn Oracle - Larry Ellison

Đoạn mã nguy hiểm đã được kiểm chứng này hi

Một hacker giấu mặt vừa mới cho công một đoạn mã nguy hiểm nhằm khai thác lỗ hổng bảo mật gần đây.

Chủ tịch tập đoàn Oracle - Larry Ellison

Đoạn mã nguy hiểm đã được kiểm chứng này hiện đã được phát tán thông qua danh sách thư điện tử Full-disclose với nội dung tiêu đề thư là "Trick or treat Larry". Rõ ràng bức thư này là muốn nhằm tới chủ tịch điều hành của tập đoàn Oracle Larry Ellison. Các chuyên gia bảo mật đã lấy một phần đoạn mã nguy hiểm này phục vụ cho mục đích kiểm tra và đã khẳng định đoạn mã này thực sự có khả năng đột nhập cơ sở dữ liệu Oracle bằng tài khoản và mật khẩu mặc định. Alexander Kornbrust, một trong những người sáng lập đồng thời là giám đốc điều hành của Red-Database-Security, cho rằng việc công bố đoạn mã nguy hiểm này thực sự là một lời cảnh tỉnh và cảnh báo rằng đoạn mã này có thể được thay đổi để gây ra nhiều hậu quả nghiêm trọng hơn. "Phiên bản đoạn mã này không hề nguy hiểm nhưng bất kỳ một ai đó cũng có thể sử dụng cái khung là đoạn mã này rồi sau đó sửa đổi thêm thắt vào sẽ có thể gây nhiều thiệt hại hơn." Kornbrust vốn là một chuyên gia rất nổi tiếng với các nghiên cứu bảo mật CSDL Oracle cũng đã tự mình tiến hành các nghiên cứu phân tích đoạn mã này và khẳng định đoạn mã này sử dụng tên đăng nhập và mật khẩu mặc định để đột nhập tấn công trong khi người quản trị phải ngồi nhìn

mà khó có thể có phản ứng gì. Đoạn mã này sử dụng UTL_TCP để gửi các lệnh điều khiển đến từng địa chỉ IP trong dải địa chỉ mạng nếu tính năng IP của hệ cơ sở dữ liệu được bật. Nếu tìm thấy một cơ sở dữ liệu thì đoạn mã này sẽ ra lệnh tạo một liên kết CSDL cá nhân và cố gắng kết nối đến đó bằng tên đăng nhập và mật khẩu mặc định. Tuy nhiên, cũng theo Kornbrust thì đoạn mã nguy hiểm này vẫn chưa "hoàn thiện" không có khả năng tự nhân bản. "Từ kinh nghiệm của tôi cho thấy, hầu hết khách hàng hiện vẫn sử dụng mật khẩu mặc định. Người sử dụng mới chỉ thay đổi mật khẩu trong một số cơ sở dữ liệu. Nhưng cũng còn đến ít nhất là 60% người sử dụng chưa hề thay đổi mật khẩu mặc định." "Nếu có một ai đó kết hợp một con sâu Windows với một con sâu tấn công Oracle thì có thể nói hậu quả sẽ khó lường. Sâu Windows có thể phát tán nhanh chóng và sẽ giúp cho sâu Oracle phát tán gây thiệt hại." Kornbrust khuyến cáo người sử dụng hay quản trị CSDL Oracle nên tiến hành những hành động sau đây: - Thay đổi mật khẩu mặc định trong mọi cơ sở dữ liệu của ứng dụng. (test/development/education/production) - Loại bỏ ưu tiên "CREATE DATABASE LINK" trong vai trò CONNECT (từ phiên bản Oracle 10g Rel.1 trở lên) - Loại bỏ cấp quyền truy cập công cộng trong gói utl_tcp. - Loại bỏ cấp quyền truy cập công cộng trong utl_inaddr. - Bảo vệ TNS bằng mật khẩu. Trong phiên bản Oracle 10g luôn luôn không kích hoạt tính năng chứng thực hệ điều hành và thay vào đó bằng mật khẩu. - Thay đổi cổng mặc định TNS từ cổng 1521 thành một cổng khác