BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

Số: 974 /CATTT-NCSC
V/v nguy cơ tấn công vào các cơ quan tổ chức qua lỗ hổng trong Oracle Weblogic

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

Hà Nội, ngày 29 tháng 10 năm 2020

Kính gửi:

- Đơn vị chuyên trách về CNTT các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước; Các Ngân hàng TMCP; Các tổ chức tài chính;
- Hệ thống các đơn vị chuyên trách về an toàn thông tin.

Trong thời gian gần đây Oracle đã công bố nhiều lỗ hổng, trong đó có lỗ hổng **CVE-2020-14882 (nghiêm trọng)** trên các máy chủ web sử dụng ứng dụng Oracle Weblogic, lỗ hổng này cho phép đối tượng tấn công vượt qua cơ chế xác thực để thực thi các đoạn mã lệnh nguy hiểm và chiếm quyền quản trị hệ thống.

Theo đánh giá sơ bộ, lỗ hổng này có thể ảnh hưởng đến nhiều cơ quan, tổ chức ở Việt Nam, đặc biệt là cơ quan chính phủ, ngân hàng, tổ chức tài chính, tập đoàn, doanh nghiệp và các công ty lớn. Có hàng trăm hệ thống thông tin của Việt Nam sử dụng ứng dụng này và đang công khai trên Internet, đây chính là những hệ thống có khả năng bị khai thác đầu tiên.

Ngày 28/10/2020 qua công tác theo dõi, giám sát an toàn thông tin, Trung tâm Giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin phát hiện có một số mã khai thác đã công khai trên Internet. Những mã khai thác này có thể sử dụng để tấn công vào máy chủ web bị ảnh hưởng, qua đó kiểm soát hệ thống thông tin của các cơ quan tổ chức.

Hiện tại, một số nhóm chuyên thực hiện tấn công APT có dấu hiệu tận dụng lỗ hổng này để tấn công sâu vào hệ thống thông tin của các cơ quan tổ chức. Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của quý đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Cục An toàn thông

tin yêu cầu đơn vị triển khai quyết liệt một số khuyến nghị sau:

1. Kiểm tra, rà soát các máy chủ web có sử dụng Oracle Weblogic để phát hiện và xử lý kịp thời nguy cơ tấn công thông qua lỗ hổng này. Trong trường hợp đã có dấu hiệu tấn công cần thực hiện rà soát toàn bộ máy chủ và hệ thống liên quan để phát hiện và loại bỏ các tập tin độc hại, mã độc mà đối tượng tấn công để lại trên hệ thống.

2. Cập nhật bản vá lỗ hổng bảo mật cho ứng dụng. Trong trường hợp chưa thể cập nhật bản vá cần triển khai các biện pháp để hạn chế, ngăn chặn việc khai thác lỗ hổng.

3.Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại: 02432091616, thư điện tử: ais@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Phạm Anh Tuấn (để b/c);
- Cục trưởng (để b/c);
- PCT Nguyễn Khắc Lịch;
- Lưu: VT, NCSC.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

Ký bởi: Cục An toàn thông tin
Cơ quan: Bộ Thông tin và Truyền thông
Thời gian ký: 29/10/2020 18:31:17

CỘNG HOÀ X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Khắc Lịch

Phụ lục
Thông tin về lỗ hổng
(kèm theo Công văn số /CATTT-NCSC ngày / /2020)

1. Thông tin chung

- Mã lỗi: CVE-2020–14882

- Điểm CVSS: 9.8 (Nghiêm trọng)

- Ảnh hưởng: Oracle WebLogic Server phiên bản 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0.

- Để khai thác lỗ hổng, đối tượng tấn công chỉ cần gửi một yêu cầu GET (trong đó có các đoạn mã lệnh độc hại) đến hệ thống là có thể thực thi các lệnh này trên hệ thống và có thể chiếm quyền điều khiển hệ thống.

2. Hướng dẫn xử lý lỗ hổng

- Cập nhật bản vá cho ứng dụng.

- Trong trường hợp chưa thể cập nhật bản vá thì có thể thực hiện một số biện pháp để hạn chế tấn công:

+ Chặn truy cập đến cổng ứng dụng (mặc định là 7001)

+ Chặn các request độc hại trên tường lửa ứng dụng web. Đoạn code để vượt qua xác thực **"%252E%252E%252F"**.