BỘ THÔNG TIN TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

Số: 2130 /CATTT-NCSC
V/v Cảnh báo về lỗ hổng an toàn thông tin tồn tại trên sản phẩm Oracle WebLogic Server

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

Hà Nội, ngày 23 tháng 10 năm 2024

Kính gửi:

- Đơn vị chuyên trách về CNTT/ATTT 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 Doanh nghiệp cung cấp dịch vụ viễn thông, Internet và nền tảng số;
- Các Tổ chức tài chính, Ngân hàng thương mại;
- Hệ thống các đơn vị chuyên trách về an toàn thông tin.

Thực hiện chức năng giám sát an toàn thông tin trên không gian mạng, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin, Bộ Thông tin và Truyền thông, đã phát hiện và ghi nhận mã khai thác của lỗ hổng **CVE-2024-21216** cho phép đối tượng tấn công chiếm quyền kiểm soát Oracle WebLogic Server. Lỗ hổng **CVE-2024-21216** được đánh giá ở mức độ nghiêm trọng, việc rà soát và nâng cấp phiên bản hoặc áp dụng biện pháp khắc phục thay thế cần được thực hiện ngay lập tức.

(Thông tin chi tiết xem tại Phụ lục kèm theo)

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 đề nghị Quý Đơn vị thực hiện:

1. Kiểm tra, rà soát hệ thống thông tin đang sử dụng có khả năng bị ảnh hưởng bởi lỗ hổng an toàn thông tin trên. Chủ động theo dõi các thông tin liên quan đến đến các chiến dịch tấn công mạng nhằm thực hiện ngăn chặn sớm, tránh nguy cơ bị tấn công.

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát

hiện kịp thời các nguy cơ tấn công mạng.

3. Gửi báo cáo kết quả rà soát hệ thống về Cục An toàn thông tin **chậm nhất trước ngày 25/10/2024**. 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, điện thoại 02432091616, thư điện tử: ncsc@ais.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Phạm Đức Long (để b/c);
- Cục A05 (Bộ Công an);
- Bộ Tư lệnh 86 (Bộ Quốc phòng);
- Ban Cơ yếu Chính phủ;
- Đơn vị chuyên trách về CNTT/ATTT của: Văn phòng Trung ương Đảng; Văn phòng Quốc hội; Văn phòng Chủ tịch nước; Tòa án nhân dân tối cao; Viện Kiểm sát nhân dân tối cao; Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam;
- Các Cục: Viễn thông, Bưu điện Trung ương;
- Trung tâm VNNIC, Trung tâm Thông tin;
- Ngân hàng Chính sách xã hội;
- Ngân hàng Phát triển Việt Nam;
- Ngân hàng Hợp tác xã Việt Nam;
- Ngân hàng Thương mại Cổ phần;
- Các công ty Cổ phần Chứng khoán;
- Các Tổ chức, doanh nghiệp hoạt động trong lĩnh vực thương mại điện tử;
- Các tổ chức, doanh nghiệp cung cấp dịch vụ trung gian thanh toán, ví điện tử;
- Cục trưởng (để b/c);
- Phó Cục trưởng Trần Quang Hưng;
- P.ATHTTT, P.QHPT, VNCERT/CC;
- Lưu: VT, NCSC.LTQ.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

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

Trần Quang Hưng

Phụ lục

THÔNG TIN CHI TIẾT VỀ LỖ HỔNG AN TOÀN THÔNG TIN

(Kèm theo Công văn số 2130/CATTT-NCSC ngày 23/10/2024

của Cục An toàn thông tin)

1. Thông tin chi tiết các chiến dịch tấn công

Trung tâm Giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin ghi nhận thông tin liên quan đến lỗ hổng CVE-2024-21216 tồn tại trên các sản phẩm của hãng Oracle.

Lỗ hổng CVE-2024-21216 (Điểm CVSS: 9.8 – Nghiêm trọng) cho phép đối tượng tấn công không cần xác thực chiếm quyền kiểm soát Oracle WebLogic Server.

Cụ thể, lỗ hổng tồn tại trên sản phẩm Oracle WebLogic Server của Oracle Fusion Middleware (thành phần: Core) bao gồm các phiên bản 12.2.1.4.0 và 14.1.1.0.0. Đối tượng tấn công có thể khai thác lỗ hổng nếu có thể tiếp cận vào hệ thống mạng, thông qua việc khai thác giao thức T3, IIOP.

Hiện lỗ hổng đã được khắc phục trong bản vá mới nhất của hãng, tuy nhiên trong trường hợp chưa thể cập nhật bản vá người dùng có thể chặn các giao thức bị khai thác bởi lỗ hổng để giảm khả năng bị ảnh hưởng bởi các nỗ lực khai thác.

2. Tài liệu tham khảo

https://www.tenable.com/cve/CVE-2024-21216