UBND TỈNH KIÊN GIANG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số : 2790 /STTTT-CĐS

Kiên Giang, ngày 30 tháng 10 năm 2024

V/v cảnh báo về lỗ hổng an toàn thông tin tồn tại trên sản phẩm Oracle WebLogic Server

Kính gửi:
- Các cơ quan Đảng, đoàn thể;
- Các sở, ban, ngành tỉnh;
- Ủy ban nhân dân các huyện, thành phố.

Sở Thông tin và Truyền thông Kiên Giang nhận được Công văn số 2130/CATTT-NCSC ngày 23/10/2024 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc cảnh báo về lỗ hổng an toàn thông tin tồn tại trên sản phẩm Oracle WebLogic Server.

Trong quá trình 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 các hệ thống thông tin của Quý Đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam. Sở Thông tin và Truyền thông Kiên Giang khuyến nghị Quý Đơn vị lưu ý thực hiện một số nội dung sau:

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.

Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ sau:

- Cục An toàn thông tin - Bộ Thông tin và Truyền thông: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ncsc@ais.gov.vn.

- Hoặc Phòng Chuyển đổi số - Sở Thông tin và Truyền thông Kiên Giang, điện thoại: 0297.3921678. thư điện tử: cds.stttt@kiengiang.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Trung tâm CNTT&TT (t/h);
- Lưu: VT, CĐS, ttnghi.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH KIÊN GIANG

Nguyễn Xuân Kiệm

PHỤ LỤC
THÔNG TIN CHI TIẾT VỀ LỖ HỔNG AN TOÀN THÔNG TIN

(Kèm theo Công văn số /STTTT-CĐS ngày / 10 /2024 của Sở Thông tin và Truyền Thông Kiên Giang)

1. Thông tin chi tiết về lỗ hổng an toàn thông tin

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