UBND TỈNH QUẢNG NGÃI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 2488 /STTTT-BCVT&CNTT

Quảng Ngãi, ngày 28 tháng 10 năm 2024

V/v cảnh báo rủi ro an toàn thông tin tin tồn tại trên sản phẩm Oracle WebLogic Server

Kính gửi:

- Văn phòng: Tỉnh ủy, Đoàn ĐBQH&HĐND, UBND tỉnh;
- Các sở, ban, ngành; Hội, đoàn thể tỉnh;
- UBND các huyện, thị xã, thành phố;
- Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Công an tỉnh;
- UBND các xã, phường, thị trấn;
- Báo Quảng Ngãi, Đài Phát thanh và Truyền hình tỉnh.

Theo cảnh báo của Cục An toàn thông tin tại Công văn số 2130/CATTT-NCSC ngày 23/10/2024 về việc Cảnh báo về lỗ hổng an toàn thông tin tồn tại trên sản phẩm Oracle WebLogic Server, Sở Thông tin và Truyền thông đề nghị lãnh đạo các cơ quan, đơn vị chỉ đạo thực hiện một số biện pháp sau để hạn chế các rủi ro về nguy cơ mất an toàn thông tin, cụ thể:

1. Kiểm tra, rà soát hệ thống thông tin đang sử dụng có khả năng bị ảnh hưởng bởi lỗ hổng **CVE-2024-21216** cho phép đối tượng tấn công chiếm quyền kiểm soát Oracle WebLogic Server. Chủ động theo dõi các thông tin liên quan nhằm thực hiện khắc phục rủi ro trong trường hợp bị ảnh hưởng.

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.

3. Khi phát hiện các hệ thống có biểu hiện bị khai thác, tấn công mạng, triển khai ngay các biện pháp xử lý ngăn chặn tấn công trên hệ thống và thông báo về Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi để có các biện pháp hỗ trợ, xử lý kịp thời.

(Gửi kèm Phụ lục Thông tin về lỗ hổng an toàn thông tin)

Đề nghị lãnh đạo các cơ quan, đơn vị quan tâm chỉ đạo thực hiện./.

***Nơi nhận*:**
- Như trên;
- UBND tỉnh (báo cáo);
- Cục An toàn thông tin (báo cáo);
- Phòng VH&TT các huyện, thị xã, thành phố;
- Thành viên Đội ứng cứu sự cố ATTT mạng tỉnh;
- Sở TT&TT: Lãnh đạo Sở, các phòng chuyên môn, TT CĐS;
- Lưu: VT, BCVT&CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH QUẢNG NGÃI

Nguyễn Quốc Huy Hoàng

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

(Kèm theo Công văn số 2488/STTTT-BCVT&CNTT ngày 28/10/2024 của Sở Thông tin và Truyền thông)

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
