UBND TỈNH QUẢNG BÌNH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 2136 /STTTT-TTCNTT
V/v cảnh báo về lỗ hổng an toàn thông tin tồn tại trên sản phẩm Oracle WebLogic Server

Quảng Bình, ngày 30 tháng 10 năm 2024

Kính gửi:

- Văn phòng Tỉnh ủy, Văn phòng Đoàn ĐBQH & HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các sở, ban, ngành, tổ chức đoàn thể cấp tỉnh;
- UBND các huyện, thị xã, thành phố.

Sở Thông tin và Truyền thông 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.

Theo đó, 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 (*Phụ lục kèm theo).*

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý cơ quan, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông đề nghị Quý cơ quan quan tâm chỉ đạo, thực hiện:

1. Kiểm tra, rà soát hệ thống thông tin đang sử dụng có khả năng bị ảnh hưởng bởi các chiến dịch tấn công 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 hỗ trợ, Quý cơ quan liên hệ Trung tâm Công nghệ thông tin và Truyền thông thuộc Sở Thông tin và Truyền thông *(Đơn vị thường trực Đội Ứng cứu sự cố an toàn thông tin mạng của tỉnh)*; điện thoại: 0232.3856696; email: ungcuusuco@quangbinh.gov.vn.

Rất mong được sự quan tâm, phối hợp của Quý cơ quan./.

Nơi nhận:
- Như trên;
- UBND tỉnh (báo cáo);
- Lãnh đạo Sở;
- Phòng CĐS;
- Lưu: VT, TTCNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Nguyễn Xuân Ngọc

Phụ lục

THÔNG TIN CHI TIẾT VỀ CHIẾN DỊCH TẤN CÔNG

(Kèm theo Công văn số 2136 */STTTT-TTCNTT, ngày 30/10/2024*
của Sở Thông tin và Truyền thông Quảng Bình)

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