UBND TỈNH TÂY NINH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 2143 /STTTT-TTGSĐH
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

Tây Ninh, ngày 28 tháng 10 năm 2024

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các cơ quan tham mưu, giúp việc Tỉnh ủy;
- Mặt trận Tổ quốc và các Đoàn thể chính trị - xã hội;
- Các Sở, ban, ngành tỉnh;
- Các đơn vị ngành dọc;
- Các huyện, thị, thành ủy trực thuộc Tỉnh ủy;
- UBND các huyện, thị xã, thành phố;
- UBND các xã, phường, thị trấn.

Thực hiện theo Công văn số 2130/CATTT-NCSC 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 ***(Thông tin chi tiết phụ lục kèm theo)***.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các đơn vị và góp phần đảm bảo an toàn thông tin trên địa bàn tỉnh, Sở Thông tin và Truyền thông đề nghị các đơn vị, địa phương thực hiện gấp các công việc cụ thể như sau:

1. Kiểm tra, rà soát hệ thống thông tin đang sử dụng có khả năng bị ảnh hưởng bởi mã độc 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 uy tín về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

Thông tin liên quan đề nghị liên hệ Ông Đào Quang Phúc - Trung tâm Giám sát, điều hành kinh tế, xã hội tập trung; Điện thoại: 0937.117.128.

Trân trọng./.

Nơi nhận:
- Như trên;
- BGĐ Sở (b/c);
- P.CNTTBCVT;
- Lưu: VT, TTGSĐH.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH TÂY NINH

Nguyễn Trung Hiếu

PHỤ LỤC
THÔNG TIN THÔNG TIN CHI TIẾT VỀ MÃ ĐỘC

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