UBND TỈNH ĐỒNG NAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 2361 /STTTT-CNTTVT
V/v 06 lỗ hổng bảo mật mới ảnh hưởng cao và nghiêm trọng trong Oracle WebLogic Server

Đồng Nai, ngày 2 tháng 8 năm 2021

Kính gửi:

- Các cơ quan đảng, nhà nước trên địa bàn tỉnh;
- Các tổ chức chính trị - xã hội thuộc địa bàn tỉnh.

Sở Thông tin và Truyền thông nhận được văn bản 993/CATTT-NCSC ngày 23/7/2021 của Cục An toàn thông tin về việc 06 lỗ hổng bảo mật mới ảnh hưởng cao và nghiêm trọng trong Oracle WebLogic Server.

Ngày 20/7/2021, Oracle đã công bố 342 bản vá trong bản phát hành các bản vá quan trọng tháng 7/2021 cho các điểm yếu, lỗ hổng trên sản phẩm của mình, đặc biệt trong đó có nhiều lỗ hổng bảo mật có mức ảnh hưởng nghiêm trọng. Nổi bật là 06 lỗ hổng bảo mật (CVE-2021-2394, CVE-2021-2397, CVE-2021-2382, CVE-2021-2378, CVE-2021-2376, CVE-2021-2403) trong sản phẩm Oracle WebLogic Server. Trong đó 03 lỗ hổng bảo mật (CVE-2021-2394, CVE-2021-2397, CVE-2021-2382) có mức ảnh hưởng nghiêm trọng, cho phép đối tượng tấn công thực thi mã từ xa mà không cần xác thực (thông tin chi tiết về các lỗ hổng có tại phụ lục kèm theo).

Theo đánh giá sơ bộ, WebLogic Server được sử dụng nhiều trong các hệ thống thông tin của các cơ quan, tổ chức ở Việt Nam, đặc biệt là cơ quan chính phủ, ngân hàng, tổ chức tài chính, tập đoàn, doanh nghiệp và các công ty lớn. Trên cơ sở đó và thực tế triển khai công tác giám sát an toàn thông tin những năm qua, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) dự báo những lỗ hổng này sẽ sớm có mã khai thác công khai trên Internet. Điều này có thể dẫn đến nguy cơ tấn công mạng trên diện rộng trong thời gian tới.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông khuyến nghị quý cơ quan, đơn vị, địa phương khẩn trương thực hiện các nội dung theo hướng dẫn sau:

1. Kiểm tra, rà soát và xác định máy chủ web có sử dụng Oracle WebLogic để phát hiện và xử lý kịp thời nguy cơ tấn công thông qua các lỗ hổng bảo mật trên và các sản phẩm khác có trong danh sách cảnh báo của Oracle có tại

https://www.oracle.com/security-alerts/cpujul2021.html. Tiến hành cập nhật bản vá lỗ hổng bảo mật cho các máy chủ bị ảnh hưởng (tham khảo hướng dẫn tại phụ lục kèm theo).

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 của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin điện thoại 024.32091616, thư điện tử: ais@mic.gov.vn; hoặc phòng Công nghệ thông tin Viễn thông - Sở Thông tin và Truyền thông, số điện thoại: 0251.8825678.

Trân trọng./.

Đính kèm: Văn bản 993/CATTT-NCSC ngày 23/7/2021 của Cục An toàn thông tin về việc 06 lỗ hổng bảo mật mới ảnh hưởng cao và nghiêm trọng trong Oracle WebLogic Server.

(Văn bản 993/CATTT-NCSC tải về tại mục an toàn thông tin mạng theo địa chỉ http://stttt.dongnai.gov.vn/Pages/news.aspx?CatId=56).

Nơi nhận:
- Như trên;
- Giám đốc và PGĐ Sở;
- Trung tâm CNTT&TT;
- Lưu: VT, CNTTVT, TienLHV.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH ĐỒNG NAI

Võ Hoàng Khai