

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

Hà Nội, ngày tháng năm 2021

Kính gửi: Các đơn vị trực thuộc Bộ có hệ thống thông tin

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, Cục An toàn thông tin 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 bảo đảm an toàn thông tin cho hệ thống thông tin của Quý đơn vị, Trung tâm Công nghệ thông tin khuyến nghị Quý đơn vị thực hiện:

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, Quý đơn vị liên hệ đầu mối hỗ trợ của Trung tâm Công nghệ thông tin: Phòng Kỹ thuật hạ tầng, điện thoại 024.39439060, thư

điện tử: phongktht@most.gov.vn.

Trân trọng./.

Nơi nhận:

- Như trên;
- Thứ trưởng Bùi Thế Duy (đề b/c);
- Công thông tin điện tử Bộ KH&CN;
- Lưu: VT, KTHT.

GIÁM ĐỐC

Hà Quốc Trung

Phụ lục
Thông tin về lỗ hổng bảo mật
(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2021 của Trung tâm
Công nghệ thông tin)

1. Thông tin về lỗ hổng bảo mật

| TT | CVE | Mô tả | Link tham khảo |
|-----------|---------------|--|--|
| 1 | CVE-2021-2394 | <ul style="list-style-type: none">- Lỗ hổng trong Oracle WebLogic Server, cho phép đối tượng tấn công truy cập trái phép, từ đó chiếm quyền điều khiển máy chủ mục tiêu.- Điểm CVSS: 9,8 (nghiêm trọng)- Ảnh hưởng: WebLogic phiên bản 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 và 14.1.1.0.0. | https://www.oracle.com/security-alerts/cpujul2021.html https://nvd.nist.gov/vuln/detail/CVE-2021-2394 |
| 2 | CVE-2021-2397 | <ul style="list-style-type: none">- Lỗ hổng trong Oracle WebLogic Server, cho phép đối tượng tấn công truy cập trái phép, từ đó chiếm quyền điều khiển máy chủ mục tiêu.- Điểm CVSS: 9,8 (nghiêm trọng)- Ảnh hưởng: WebLogic phiên bản 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 và 14.1.1.0.0. | https://www.oracle.com/security-alerts/cpujul2021.html https://nvd.nist.gov/vuln/detail/CVE-2021-2397 |
| 3 | CVE-2021-2382 | <ul style="list-style-type: none">- Lỗ hổng trong Oracle WebLogic Server, cho phép đối tượng tấn công truy cập trái phép, từ đó chiếm quyền điều khiển máy chủ mục tiêu.- Điểm CVSS: 9,8 (nghiêm trọng)- Ảnh hưởng: WebLogic phiên bản 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 và 14.1.1.0.0. | https://www.oracle.com/security-alerts/cpujul2021.html https://nvd.nist.gov/vuln/detail/CVE-2021-2382 |

| | | | |
|---|---------------|--|--|
| 4 | CVE-2021-2378 | <ul style="list-style-type: none"> - Lỗ hổng trong Oracle WebLogic Server, cho phép đối tượng tấn công truy cập trái phép máy chủ mục tiêu. - Điểm CVSS: 7.5 (cao) - Ảnh hưởng: phiên bản 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0 | https://www.oracle.com/security-alerts/cpujul2021.html https://nvd.nist.gov/vuln/detail/CVE-2021-2378 |
| 5 | CVE-2021-2376 | <ul style="list-style-type: none"> - Lỗ hổng trong Oracle WebLogic Server, cho phép đối tượng tấn công truy cập trái phép máy chủ mục tiêu. - Điểm CVSS: 7.5 (cao) - Ảnh hưởng: phiên bản 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0. | https://www.oracle.com/security-alerts/cpujul2021.html https://nvd.nist.gov/vuln/detail/CVE-2021-2376 |
| 6 | CVE-2021-2403 | <ul style="list-style-type: none"> - Lỗ hổng trong Oracle WebLogic Server, cho phép đối tượng tấn công truy cập trái phép máy chủ mục tiêu. - Điểm CVSS: 5.3 (trung bình) - Ảnh hưởng: phiên bản 10.3.6.0.0, 12.1.3.0.0. | https://www.oracle.com/security-alerts/cpujul2021.html https://nvd.nist.gov/vuln/detail/CVE-2021-2403 |

2. Hướng dẫn khắc phục

Cách tốt nhất để khắc phục các lỗ hổng bảo mật này là cập nhật bản vá theo hướng dẫn của Oracle. Tại thời điểm này, Oracle chưa có công bố về các biện pháp khắc phục thay thế để giảm thiểu nguy cơ tấn công. Vì vậy, Quý đơn vị cần thực hiện cập nhật bản vá trong thời gian sớm. Tham khảo thông tin các bản vá tại: <https://www.oracle.com/security-alerts/cpujul2021.html>

DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN

(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2021 của Trung tâm Công nghệ thông tin)

| TT | Tên đơn vị |
|-----------|--|
| 1. | Tổng Cục tiêu chuẩn đo lường chất lượng |
| 2. | Cục Thông tin Khoa học và Công nghệ Quốc gia |
| 3. | Cục An toàn bức xạ và hạt nhân |
| 4. | Cục Sở hữu trí tuệ |
| 5. | Ban quản lý khu công nghệ cao Hoà Lạc |
| 6. | Học viện Khoa học, Công nghệ và Đổi mới sáng tạo |
| 7. | Viện Năng lượng nguyên tử Việt Nam |
| 8. | Viện Khoa học sở hữu trí tuệ |
| 9. | Quỹ Phát triển khoa học và công nghệ quốc gia |
| 10. | Quỹ Đổi mới công nghệ quốc gia |