Phụ lục

THÔNG TIN VỀ LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số /STTTT-TTCNTT&TT ngày /11/2020 của Sở Thông tin và Truyền thông)

1. Thông tin chung lỗ hổng bảo mật

STT	Các phiên bản Oracle WebLogic Server	CVE	Điểm CVSS
1	10.3.6.0.0	2020–14882	9.8 (nghiêm trọng)
2	12.1.3.0.0		
3	12.2.1.3.0		
4	12.2.1.4.0		
5	14.1.1.0.0		

Để khai thác lỗ hổng, đối tượng tấn công chỉ cần gửi một yêu cầu GET (trong đó có các đoạn mã lệnh độc hại) đến hệ thống là có thể thực thi các lệnh này trên hệ thống và có thể chiếm quyền điều khiển hệ thống.

2. Hướng dẫn khắc phục lỗ hổng bảo mật

- Cập nhật bản vá cho ứng dụng.

- Trong trường hợp chưa thể cập nhật bản vá thì có thể thực hiện một số biện pháp để hạn chế tấn công:

+ Chặn truy cập đến cổng (port) ứng dụng (mặc định là 7001)

+ Chặn các request độc hại trên tường lửa ứng dụng web. Đoạn code để vượt qua xác thực **“%252E%252E%252F”**.

---Hết---