UBND TỈNH NINH BÌNH
SỞ NÔNG NGHIỆP VÀ PTNT

Số: 2617 /SNN-VP
V/v triển khai rà quét, khắc phục nguy cơ tấn công mạng vào các cơ quan, tổ chức qua lỗ hổng trong Oracle Weblogic

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

Ninh Bình, ngày 16 *tháng* 11 *năm 2020*

Kính gửi: Các đơn vị trực thuộc Sở

Sở Nông nghiệp và Phát triển nông thôn nhận được Văn bản số 1540/STTTT-CNTT ngày 06/11/2020 của Sở Thông tin và Truyền thông về việc triển khai rà quét, khắc phục nguy cơ tấn công mạng vào các cơ quan, tổ chức qua lỗ hổng trong Oracle Weblogic.

Trong thời gian gần đây Oracle đã công bố nhiều lỗ hổng, trong đó có lỗ hổng **CVE-2020-14882** trên các máy chủ web sử dụng ứng dụng Oracle Weblogic, lỗ hổng này cho phép đối tượng tấn công vượt qua cơ chế xác thực để thực thi các đoạn mã lệnh nguy hiểm và chiếm quyền quản trị hệ thống.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các đơn vị trực thuộc Sở, Sở Nông nghiệp và Phát triển nông thôn yêu cầu các đơn vị triển khai thực hiện một số nội dung sau:

1. Kiểm tra rà soát, xác minh các máy chủ web có sử dụng Oracle Weblogic để phát hiện xử lý kịp thời nguy cơ tấn công mạng qua lỗ hổng trên. Trường hợp phát hiện dấu hiệu tấn công cần thực hiện rà soát toàn bộ máy chủ và loại bỏ các tập tin độc hại, mã độc mà đối tượng tấn công để lại trên hệ thống.

2. Cập nhật bản vá lỗ hổng bảo mật cho ứng dụng *(Hướng dẫn cập nhật chi tiết tại Phụ lục gửi kèm)*. Trong trường hợp chưa thể cập nhật bản vá cần triển khai các biện pháp để hạn chế, ngăn chặn việc khai thác lỗ hổng.

Trong quá trình thực hiện nếu cần hỗ trợ đề nghị liên hệ: Ông Quách Hoàng Thạch, Quản trị mạng - Văn phòng Sở, điện thoại: 0915.386.012.

Sở Nông nghiệp và Phát triển nông thôn yêu cầu các đơn vị nghiêm túc thực hiện các nội dung trên./.

Nơi nhận:
- Như trên;
- Lãnh đạo Sở (để b/c);
- Trang Thông tin điện tử của Sở;
- Lưu: VT, VP.

MC

TL.GIÁM ĐỐC
CHÁNH VĂN PHÒNG

Ký bởi: Sở Nông nghiệp và Phát triển Nông thôn
Cơ quan: Tỉnh Ninh Bình
Thời gian ký: 16/11/2020 08:29:37

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ NÔNG NGHIỆP VÀ PHÁT TRIỂN NÔNG THÔN
TỈNH NINH BÌNH

Bùi Xuân Thư

Phụ lục

HƯỚNG DẪN CHI TIẾT VÁ LỖ HỔNG BẢO MẬT ORACLE WEBLOGIC

(Kèm theo Văn bản số 2617*/SNN-VP ngày* 16*/*11*/2020 của Sở Nông nghiệp và PTNT)*

1. Thông tin chung

- Mã lỗi: CVE-2020-14882.

- Điểm Lỗ hổng ghi hệ thống chung (CVSS): 9.8 (Nghiêm trọng).

- Ảnh hưởng: Oracle Weblogic Server 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.

- 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 xử lý lỗ hổng

- 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 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”.**