UBND TỈNH TUYÊN QUANG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh Phúc

Số: 370/STTTT-CNTT&BCVT
V/v dự báo nguy cơ tấn công vào hệ thống thông tin của các cơ quan, tổ chức thông qua lỗ hổng bảo mật Spring4Shell

Tuyên Quang, ngày 12 tháng 4 năm 2022

Kính gửi:
- Văn phòng Hội đồng nhân dân tỉnh;
- Văn phòng Ủy ban nhân dân tỉnh;
- Các sở, ban, ngành;
- Uỷ ban nhân dân các huyện, thành phố;
- Trung tâm Công nghệ thông tin và Truyền thông, Sở Thông tin và Truyền thông.

Căn cứ văn bản số 430/CATTT – NCSC ngày 31/3/2022 của Cục An toàn thông tin về việc dự báo nguy cơ tấn công vào hệ thống thông tin của các cơ quan, tổ chức thông qua lỗ hổng bảo mật Spring4Shell;

Sở Thông tin và Truyền thông cảnh báo tới các cơ quan, đơn vị, thông tin cụ thể như sau:

I. Thông tin về lỗ hổng bảo mật trong các sản phẩm Microsoft

Ngày 30/3/2022 vừa qua, mã khai thác của một lỗ hổng bảo mật (có tên gọi Spring4Shell) đã được công khai trên Internet trong khi lỗ hổng này còn chưa có mã lỗi quốc tế (CVE) đồng thời chưa có bản vá. Lỗ hổng này tồn tại trong Spring Core, một thành phần lõi trong bộ mã nguồn mở Spring Framework được sử dụng phổ biến trong các ứng dụng hiện nay, ảnh hưởng đến ứng dụng sử dụng Spring Core với phiên bảnJDK >=9.0, cho phép đối tượng tấn công thực thi mã từ xa và kiểm soát hệ thống.

Theo một số khảosát đã công bố, có tới hơn 30% sản phẩm được viết bằng Java có sử dụng Spring Core, ngoài ra đến nay vẫn chưa có thông tin về bản vá chính thức từ nhà phát triển để khắc phục lỗ hổng nên mức độ ảnh hưởng của lỗ hổng này được đánh giá rất **Nghiêm trọng**. Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) ghi nhận mã khai thác đã được công bố trên Internet và dự báo lỗ hổng này sẽ được các nhóm tấn công có chủ đích (APT) tận dụng để thực hiện các cuộc tấn công nguy hiểm trên diện rộng ngay lập tức.

Qua quá trình giám sát, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) cũng phát hiện dấu hiệu dò quét và khai thác thử vào một số hệ thống công nghệ thông tin của các cơ quan, tổ chức tại Việt Nam thông qua lỗ hổng này.

(Thông tin chi tiết các lỗ hổng bảo mật có tại phụ lục kèm theo).

II. Các giải pháp phòng tránh

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý cơ quan đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông đề nghị các sở, ban, ngành, Ủy ban nhân dân các huyện, thành phố triển khai thực hiện:

1. Kiểm tra, rà soát và xác minh hệ thống thông tin có sử dụng Spring core. Trong trường hợp bị ảnh hưởng, Quý đơn vị cần thực hiện các biện pháp khắc phục thay thế trong thời gian chờ bản vá được phát hành; đồng thời nâng cấp các ứng dụng và thành phần liên quan có khả năng bị ảnh hưởng.

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.

3. Trong trường hợp cần hỗ trợ, Quý đơn vị liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại: 02432091616, thư điện tử: ncsc@ais.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Ban Giám đốc sở (báo cáo);
- Lưu: VT, CNTT&BCVT

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH TUYÊN QUANG

Nguyễn Văn Hiến

Phụ lục

Thông tin về các lỗ hổng bảo mật

(Kèm theo Công văn số/STTTT-CNTT&BCVT ngày 12 /4/2022 của Sở Thông tin và Truyền thông)

1. Thông tin lỗ hổng bảo mật

- **Mô tả**: Lỗ hổng này tồn tại trong Spring Core, cho phép đối tượng tấn công thực thi mã từ xa.

- **Ảnh hưởng**:ứng dụng sử dụng Spring Core phiên bản JDK >= 9.0.

2. Hướng dẫn kiểm tra và khắc phục lỗ hổng

2.1. Hướng dẫn kiểm tra, xác định bị ảnh hưởng bởi lỗ hổng Srping4Shell

Bước 1: Kiểm tra phiên bản JDK

Trên máy chủ, hãy chạy lệnh "java -version" để kiểm tra phiên bản JDK đang chạy. Nếu phiên bản <= 8.0, hệ thống Quý đơn vị không bị ảnh hưởng bởi lỗ hổng này.

Bước 2: Kiểm tra việc sử dụng Spring Framework

1. Đối với hệ thống được triển khai dưới dạng war package:

- Giải nén war package

- Tìm kiếm tệp jar ở định dạng spring-beans-*.jar (ví dụ: spring-beans-5.3.16.jar) trong tệp giải nén. Nếu có tồn tại, nghĩa là hệ thống đang sử dụng Springframework.

2. Đối với hệ thống được triển khai dưới dang jar package:

- Giải nén jar package

- Tìm kiếm tệp jar ở định dạng spring-beans-*.jar (ví dụ: spring-beans-5.3.16.jar) trong tệp giải nén. Nếu có tồn tại, nghĩa là hệ thống đang sử dụng Spring framework.

- Nếu không tìm thấy tệp spring-beans-*.jar, hãy tiếp tục tìm kiếm tệp CachedIntrospectionResults.class trong tệp giải nén. Nếu tồn tại tệp này chứng tỏ hệ thống đang sử dụng Spring framework.

Bước 3: Phân tích, điều tra xác nhận

Sau khi hoàn thành 2 bước kiểm tra ở trên, các điều kiện sau được đáp ứng đồng thời sẽ xác định hệ thống bị ảnh hưởng bởi lỗ hổng bảo mật này:

- Phiên bản JDK >= 9.0

- Sử dụng Spring framework hoặc derived framework.

- Tồn tại endpoint sử dụng chức năng DataBinder.

2.2. Hướng dẫn khắc phục

Hiện tại, chưa có bản vá để khắc phục lỗ hổng bảo mật nói trên. Vì vậy, để giảm thiểu nguy cơ bị tấn công, Quý đơn vị có thể thực hiện các biện pháp khắc phục theo nguồn hướng dẫn tham khảo của một số tổ chức tại:

https://www.cyberkendra.com/2022/03/springshell-rce-0-day-vulnerability.html

3. Nguồn tham khảo

https://www.cyberkendra.com/2022/03/springshell-rce-0-day-vulnerability.html

https://www.cyberkendra.com/2022/03/spring4shell-details-and-exploit-code.html