BỘ KHOA HỌC VÀ CÔNG NGHỆ
**TRUNG TÂM CÔNG NGHỆ THÔNG TIN**

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

Số: 98 /TTCNTT-KTHT
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

*Hà Nội, ngày 05 tháng 04 năm 2022*

Kính gửi: Các đơn vị trực thuộc Bộ

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 bản JDK >=9.0, cho phép đối tượng tấn công thực thi mã từ xa và kiểm soát hệ thống.

Theo một số khảo sát 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, Cục An toàn thông tin – Bộ Thông tin và Truyền thông 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.

Do vậy, nhằm đảm bảo 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 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.

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 (để b/c);
- Cổng thông tin điện tử Bộ KH&CN;
- Lưu: VT, KTHT.

**GIÁM ĐỐC**

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

**Hà Quốc Trung**

**Phụ lục**

**THÔNG TIN LỖ HỔNG BẢO MẬT**

*(Kèm theo Công văn số 98 /TTCNTT-KTHT ngày 05 /04 /2022 của Trung tâm Công nghệ thông tin)*

## 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 Spring framework.

2. Đối với hệ thống được triển khai dưới dạng 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

**DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN**

*(Kèm theo Công văn số 98 /TTCNTT-KTHT ngày 05 /04 /2022 của Trung tâm Công nghệ thông tin)*

| TT | Tên đơn vị |
|---|---|
| 1. | Thanh tra Bộ |
| 2. | Cục Công tác phía Nam |
| 3. | Cục Ứng dụng và phát triển công nghệ |
| 4. | Cục Năng lượng nguyên tử |
| 5. | Cục Thông tin Khoa học và Công nghệ Quốc gia |
| 6. | Cục Phát triển thị trường và doanh nghiệp khoa học và công nghệ |
| 7. | Cục An toàn bức xạ và hạt nhân |
| 8. | Cục Sở hữu trí tuệ |
| 9. | Tổng Cục tiêu chuẩn đo lường chất lượng |
| 10. | Ban quản lý khu công nghệ cao Hoà Lạc |
| 11. | Học viện Khoa học, Công nghệ và Đổi mới sáng tạo |
| 12. | Viện Khoa học và công nghệ Việt Nam - Hàn Quốc (VKIST) |
| 13. | Viện Nghiên cứu sáng chế và Khai thác công nghệ |
| 14. | Viện Năng lượng nguyên tử Việt Nam |
| 15. | Viện Ứng dụng công nghệ |
| 16. | Viện Đánh giá khoa học và Định giá công nghệ |
| 17. | Viện Khoa học sở hữu trí tuệ |
| 18. | Viện Nghiên cứu và Phát triển Vùng |
| 19. | Văn phòng các Chương trình trọng điểm cấp nhà nước |
| 20. | Văn phòng Công nhận chất lượng |
| 21. | Văn phòng Đăng ký hoạt động khoa học và công nghệ |
| 22. | Văn phòng các Chương trình khoa học và công nghệ quốc gia |
| 23. | Báo Khoa học và Phát triển |
| 24. | Tạp chí Khoa học và Công nghệ Việt Nam |
| 25. | Nhà xuất bản Khoa học và Kỹ thuật |
| 26. | Quỹ Phát triển khoa học và công nghệ quốc gia |
| 27. | Quỹ Đổi mới công nghệ quốc gia |
| 28. | Trung tâm Nghiên cứu và Phát triển truyền thông khoa học và công nghệ |
| 29. | Trung tâm Nghiên cứu và Phát triển hội nhập khoa học và công nghệ quốc tế |