

Số: 1145 /STTTT-CNTT-VT

Đồng Nai, ngày 18 tháng 5 năm 2022

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

Kính gửi:

- Các cơ quan đảng, nhà nước trên địa bàn tỉnh;
- Các tổ chức chính trị - xã hội thuộc địa bàn tỉnh ;
- Viettel Đồng Nai, VNPT Đồng Nai, Mobifone Đồng Nai;
- Trung tâm Công nghệ thông tin tỉnh Đồng Nai.

Sở Thông tin và Truyền thông nhận văn bản 430/CATTT-NCSC ngày 31/3/2022 của Cục An toàn thông tin về việc nguy cơ tấn công vào hệ thống thông tin của các cơ quan, tổ chức thông qua lỗ hổng bảo mật CVE-2022-29464;

Theo văn bản trên, 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, 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.

Để tăng cường đảm bảo an toàn thông tin mạng trên địa bàn tỉnh, góp phần bảo đảm bảo an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông đề nghị Quý đơn vị chủ động thực hiện các biện pháp sau:

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 hoặc Sở Thông tin và Truyền thông, điện thoại 0251.3810.269, thư điện tử: attt@dongnai.gov.vn.

Trân trọng./.

Nơi nhận:

- Như trên;
- UBND tỉnh (b/c);
- Giám đốc và Phó Giám đốc Sở;
- Lưu: VT, CNTT, Thịnh.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Võ Hoàng Khai

Phụ lục
THÔNG TIN LỖ HỔNG BẢO MẬT
(Kèm theo văn bản số **1145/STTTT-CNTT**VT ngày **18/5/2022** 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 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 \geq 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>