

UBND TỈNH GIA LAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 522/STTTT-CNTT
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

Gia Lai, ngày 06 tháng 4 năm 2022

Kính gửi:

- Công an tỉnh;
- Bộ Chỉ huy Quân sự tỉnh;
- Bộ Chỉ huy Bộ đội biên phòng tỉnh;
- Văn phòng Đoàn đại biểu Quốc hội và Hội đồng nhân dân tỉnh;
- Văn phòng Ủy ban Mặt trận tổ quốc Việt Nam tỉnh;
- Các sở, ban, ngành thuộc tỉnh;
- Các hội, đoàn thể tỉnh;
- Ủy ban nhân dân các huyện, thị xã, thành phố;
- Trung tâm CNTT&TT tỉnh Gia Lai.

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 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.

Thực hiện khuyến nghị của Cục An toàn thông tin tại Công văn số 430/CATTT-NCSC ngày 31/3/2022 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 tỉnh Gia Lai đề nghị các đơn vị, địa phương kiểm tra, rà soát, khắc phục kịp thời lỗ hổng bảo mật Spring4Shell, cụ thể như sau:

1. Kiểm tra, rà soát, xác minh hệ thống thông tin có sử dụng Spring core để có phương án xử lý, khắc phục lỗ hổng. 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 lỗ hổng bảo mật Spring4Shell (*Hướng dẫn chi tiết trong Phụ lục đính kèm*).

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.

Sở Thông tin và Truyền thông tỉnh Gia Lai đề nghị các đơn vị, địa phương phối hợp, triển khai thực hiện./.

Nơi nhận:

- Như trên;
- UBND tỉnh (báo cáo);
- Cục An toàn thông tin;
- Văn phòng Tỉnh ủy;
- Lưu: VT, P. CNTT.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Đặng Quang Khanh

Phụ lục:

THÔNG TIN VỀ LỖ HỔNG BẢO MẬT SPRING4SHELL VÀ HƯỚNG DẪN XỬ LÝ, KHẮC PHỤC LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số: 522/STTTT-CNTT ngày 06 tháng 4 năm 2022
của Sở Thông tin và Truyền thông tỉnh Gia Lai)

1. Thông tin các 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 của 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, các đơn vị, địa phương có thể thực hiện các biện pháp khắc phục theo nguồn hướng dẫn tham khảo của một số tổ chức tại địa chỉ sau:

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

3. Tài liệu 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>*