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: 2309/STTTT-CNTT
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng nghiêm trọng trong Apache Log4j

Gia Lai, ngày 14 tháng 12 năm 2021

Kính gửi:

- Công an tỉnh;
- Bộ Chỉ huy Quân sự tỉnh;
- Bộ Chỉ huy Bộ đội biên phòng tỉnh;
- Văn phòng Tỉnh ủy;
- 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 09/12/2021 vừa qua, mã khai thác của lỗ hổng tồn tại trong Apache Log4j đã được công khai rộng rãi trên Internet. Lỗ hổng này ảnh hưởng đến Apache Log4j phiên bản từ 2.0 đến 2.14.1, cho phép đối tượng tấn công thực thi mã từ xa. Apache Log4j là một thư viện ghi log trong Java, tồn tại trong nhiều ứng dụng hiện nay được sử dụng phổ biến trong các hệ thống thông tin của cơ quan, tổ chức và doanh nghiệp. Vì vậy, theo đánh giá của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin, lỗ hổng này khá nghiêm trọng và có mức độ ảnh hưởng lớn.

Thực hiện khuyến nghị của Cục An toàn thông tin tại Công văn số 1734/CATTT-NCSC ngày 10/12/2021 về việc lỗ hổng bảo mật ảnh hưởng nghiêm trọng trong Apache Log4j; 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 ảnh hưởng nghiêm trọng trong Apache Log4j, cụ thể như sau:

1. Kiểm tra, rà soát và xác minh hệ thống thông tin có sử dụng Apache Log4j (thư viện ghi log trong Java) để có phương án xử lý, khắc phục lỗ hổng. Thực hiện cập nhật lên phiên bản mới nhất (log4j-2.15.0-rc2) để tránh nguy cơ bị tấn công, đồng thời nâng cấp các ứng dụng và thành phần liên quan có khả năng bị ảnh hưởng như srping-boot-strater-log4j2, Apache Solr, Apache Flink, Apache2 Druid,… (*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;
- Lưu: VT, P. CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH GIA LAI

Đặng Quang Khanh

Phụ lục:

THÔNG TIN VỀ LỖ HỔNG BẢO MẬT ẢNH HƯỞNG NGHIÊM TRỌNG TRONG APACHE LOG4J VÀ HƯỚNG DẪN XỬ LÝ, KHẮC PHỤC LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số: 2309/STTTT-CNTT ngày 14 tháng 12 năm 2021 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 Apache Log4j2, cho phép đối tượng tấn công thực thi mã từ xa.

- Ảnh hưởng: Lỗ hổng này ảnh hưởng đến Apache Log4j phiên bản từ 2.0 đến 2.14.1. Các ứng dụng và thành phần dễ bị ảnh hưởng srping-boot-strater-log4j2, Apache Solr, Apache Flink, Apache Druid.

2. Hướng dẫn khắc phục:

Thực hiện cập nhật lên phiên bản mới nhất (log4j-2.15.0-rc2). Tham khảo thông tin tại: *https://github.com/apache/logginglog4j2/releases/tag/log4j-2.15.0-rc2*

Trong trường hợp chưa thể cập nhật lên phiên bản mới nhất, có thể sử dụng biện pháp khắc phục thay thế bằng cách thêm –Dlog4j2.formatMsgNoLookups=true trong JVM args.

3. Tài liệu tham khảo:

- *https://github.com/apache/logging-log4j2/commit/*

bac0d8a35c7e354a0d3f706569116dff6c6bd658

- *https://twitter.com/P0rZ9/status/1468949890571337731*

- *https://www.lunasec.io/docs/blog/log4j-zero-day*