BỘ THÔNG TIN TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

Số: 1734 /CATTT-NCSC
V/v lỗ hổng bảo mật ảnh hưởng nghiêm trọng trong Apache Log4j

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

Hà Nội, ngày 10 tháng 12 năm 2021

Kính gửi:

- Đơn vị chuyên trách về CNTT các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước; Các Ngân hàng TMCP; Các tổ chức tài chính;
- Hệ thống các đơn vị chuyên trách về an toàn thông tin.

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 lớn. 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.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, góp phần bảo đảm bảo an toàn cho không gian mạng Việt Nam, Cục An toàn thông tin khuyến nghị Quý đơn vị thực hiện:

1. Kiểm tra, rà soát và xác minh hệ thống thông tin có sử dụng Apache Log4j. Quý đơn vị cần cập nhật lên phiên bản mới nhất (log4j-2.15.0-rc2) để khắc phục lỗ hổng bảo mật nói trên cũng như các lỗ hổng bảo mật mới phát hiện khác; đồng thời nâng cấp các ứng dụng và thành phần liên quan có khả năng bị ảnh hưởng (ví dụ như srping-boot-strater-log4j2, Apache Solr, Apache Flink, Apache

Druid,…).

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;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Huy Dũng (để b/c);
- Cục A05, Bộ Công an;
- Bộ Tư lệnh 86, Bộ Quốc phòng;
- Ban Cơ yếu Chính phủ;
- Cục trưởng;
- Lưu: VT, NCSC.

CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Thành Phúc

Phụ lục

THÔNG TIN LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số /CATTT-NCSC ngày / /2021 của Cục An toàn thông tin)

1. Thông tin 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: 2.0 <= Apache log4j <= 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

Biện pháp tốt nhất để khắc phục lỗ hổng này nâng cấp lên phiên bản mới nhất (log4j-2.15.0-rc2). Tham khảo thông tin tại: https://github.com/apache/logging-log4j2/releases/tag/log4j-2.15.0-rc2.

Trong trường hợp chưa thể nâng cấp, Quý đơn vị có thể sử dụng biện pháp khắc phục thay thế bằng cách thêm –Dlog4j2.formatMsgNoLookups=true trong JVM args.

3. Nguồn 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/