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

Số: 389 /TTCNTT-KTHT
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 16 tháng 12 năm 2021

Kính gửi: Các đơn vị trực thuộc Bộ có hệ thống 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. Theo đánh giá của Cục An toàn thông tin – Bộ Thông tin và Truyền thông, lỗ hổng này khá nghiêm trọng và có mức độ ảnh hưởng lớn.

Nhằm bảo đảm 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 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.

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 CÔNG NGHỆ TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Hà Quốc Trung

Phụ lục
Thông tin lỗ hổng bảo mật
(Kèm theo Công văn số 389/TTCNTT-KTHT ngày 16 /12 /2021 của Trung tâm Công nghệ 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. Danh sách các hãng có sản phẩm bị ảnh hưởng:

https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592#file-20211210-tlp-white_log4j-md

3. Danh sách IP/Tên miền độc hại cho đến thời điểm hiện tại:

https://hominido.medium.com/iocs-para-log4shell-rce-0-day-cve-2021-44228-98019dd06f35

4. 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.

5. Nguồn tham khảo

- https://github.com/apache/logging-log4j2/commit/bac0d8a35c7e354a0d3f706569116dff6c6bd658

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

DANH SÁCH CÁC ĐƠN VỊ CÓ HỆ THỐNG CNTT

(Kèm theo Công văn số 389/TTCNTT-KTHT ngày 16 /12 /2021 của Trung tâm Công nghệ thông tin)

TT	Tên đơn vị
1.	Tổng cục Tiêu chuẩn Đo lường Chất lượng
2.	Cục Thông tin Khoa học và Công nghệ Quốc gia
3.	Cục An toàn bức xạ và hạt nhân
4.	Cục Sở hữu trí tuệ
5.	Ban quản lý khu công nghệ cao Hoà Lạc
6.	Học viện Khoa học, Công nghệ và Đổi mới sáng tạo
7.	Viện Năng lượng nguyên tử Việt Nam
8.	Viện Khoa học sở hữu trí tuệ
9.	Quỹ Phát triển khoa học và công nghệ quốc gia
10.	Quỹ Đổi mới công nghệ quốc gia