BỘ Y TẾ
CỤC CÔNG NGHỆ THÔNG TIN

Số: 32 /CNTT-YTĐT

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 12 *tháng* 01 *năm 2022*

Kính gửi:

- Vụ, Cục, Tổng cục, Văn phòng Bộ, Thanh tra Bộ;
- Các đơn vị trực thuộc Bộ Y tế;
- Các Sở Y tế.

Cục Công nghệ thông tin nhận được công văn 1734 /CATTT-NCSC ngày 10/12/2021 của Cục An toàn thông tin về việc lỗ hổng bảo mật ảnh hưởng nghiêm trọng trong Apache Log4j.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, Cục Công nghệ thông tin trân trọng đề nghị Quý đơn vị:

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 Trung tâm Dữ liệu y tế, Cục Công nghệ thông tin, Bộ Y tế (ThS. Hoàng Đăng Trị, điện thoại: 0987772483; Email: trihd.cntt@moh.gov.vn) để được hỗ trợ.

Trân trọng./.

Nơi nhận:
- Như trên;
- Trung tâm Dữ liệu y tế (để thực hiện);
- Lưu: VT, CNTT.

CỤC TRƯỞNG

CỤC CÔNG NGHỆ THÔNG TIN

Đỗ Trường Duy

BỘ Y TẾ **CỤC CÔNG NGHỆ THÔNG TIN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**

THÔNG TIN LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số /CNTT-YTĐT ngày / /2022
của Cục 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. 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 - https://www.fortiguard.com/psirt/FG-IR-21-181

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/