UBND TỈNH THỪA THIÊN HUẾ
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 3002/STTTT-IOC
V/v cảnh báo lỗ hổng bảo mật ảnh hưởng nghiêm trọng trong Apache Log4j

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh Phúc

Thừa Thiên Huế, ngày 23 tháng 12 năm 2021

Kính gửi:
- Văn phòng Tỉnh ủy;
- Văn phòng UBND tỉnh;
- Các cơ quan chuyên môn thuộc UBND tỉnh;
- Các đơn vị sự nghiệp thuộc tỉnh;
- UBND các huyện, thị xã và thành phố Huế.

Sở Thông tin và Truyền thông nhận được Công văn số 5232/BTTTT-CATTT ngày 21/12/2021 của Bộ Thông tin và Truyền thông Về việc rà soát, xử lý lỗ hổng Log4Shell gây ảnh hưởng nghiêm trọng trên diện rộng; Công văn số 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.

Đầu tháng 12, lỗ hổng bảo mật trong Apache Log4j (còn gọi là Log4Shell có mã lỗi CVE-2021-44228) đã gây ảnh hưởng đến rất nhiều hệ thống thông tin của các tổ chức tại nhiều quốc gia trên thế giới trong đó có Việt Nam. Lỗ hổng bảo mật này đã được các chuyên gia và hãng bảo mật nhận định là lỗ hổng gây ảnh hưởng trên diện rộng và nguy hiểm nhất trong khoảng 10 năm qua. 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.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, Sở Thông tin và Truyền thông kính đề nghị quý đơn vị chủ động thực hiện:

1. Kiểm tra, rà soát và xác minh hệ thống thông tin có sử dụng Apache Log4j (đặc biệt lưu ý đối với các ứng dụng tự phát triển bằng Java). 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,…). Đối với các hệ thống, sản phẩm bị ảnh hưởng nhưng chưa có bản vá, giải pháp khắc phục từ nhà sản xuất cần thực hiện các giải pháp thay thế để đảm bảo hệ thống không bị tấn công, khai thác thông qua lỗ hổng bảo mật trên.

2. Rà soát, giám sát các dấu hiệu liên quan đến các hành vi khai thác lỗ hổng Log4Shell trên toàn bộ hệ thống thông tin để phát hiện và xử lý kịp thời các dấu hiệu tấn công mạng.

3. 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 Sở Thông tin và Truyền thông, 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.

Trân trọng./.

Nơi nhận:
- Như trên;
- UBND tỉnh (để bc);
- PA05-Công an tỉnh;
- Cổng TTĐT tỉnh;
- BGĐ Sở;
- Lưu: VT, P. CNTT, IOC.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
T. THỪA THIÊN HUẾ

Nguyễn Dương Anh

Phụ lục

THÔNG TIN LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số 3002/STTTT-IOC ngày 23 / 12 /2021 của Sở Thông tin và Truyền thông tỉnh Thừa Thiên Huế)

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/