BỘ THÔNG TIN VÀ TRUYỀN THÔNG	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 5232 /BTTTT-CATTT V/v rà soát, xử lý lỗ hổng Log4Shell gây ảnh hưởng nghiêm trọng trên diện rộng	*Hà Nội, ngày 21 tháng 12 năm 2021*

Kính gửi:

- Các Bộ, Cơ quan ngang Bộ, Cơ quan thuộc Chính phủ;
- Văn phòng Trung ương Đảng, Văn phòng Chủ tịch nước, Văn phòng Quốc hội, Tòa án nhân dân tối cao, Viện Kiểm sát nhân dân tối cao, Kiểm toán Nhà nước;
- UBND các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn kinh tế, Tổng công ty Nhà nước, các Ngân hàng TMCP; các Tổ chức tài chính.

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.

Để phản ứng trước nguy cơ đó, nhiều quốc gia trên thế giới đã yêu cầu gấp các cơ quan và tổ chức của quốc gia mình thực hiện rà soát và khắc phục đối với các hệ thống bị ảnh hưởng ngay lập tức.

Tại Việt Nam, ngày 10/12/2021 Cục An toàn thông tin đã sớm có văn bản cảnh báo số 1734/CATTT-NCSC về việc lỗ hổng bảo mật ảnh hưởng nghiêm trọng trong Apache Log4j, tuy nhiên nhiều cơ quan tổ chức vẫn còn chủ quan chưa thực hiện các biện pháp quyết liệt để xử lý lỗ hổng dẫn đến các nguy cơ gây mất an toàn thông tin ngay trước mắt. Trong khi đó, hiện nay đã có trên 400 hãng, nhà cung cấp sản phẩm, phần mềm xác nhận có sử dụng bộ thư viện Apache Log4j và bị ảnh hưởng bởi lỗ hổng trên. Trong đó có rất nhiều các hãng lớn, phổ biến được sử dụng rộng rãi tại Việt Nam như Elastic, VMware, SolarWinds, Apache Struts, Apache Solr, Jitsi...

Trước các nguy cơ đặc biệt nghiêm trọng và ảnh hưởng trên diện rộng tới phần lớn các hệ thống thông tin, nhằm đảm bảo an toàn thông tin cho các hệ thống

thông tin của Việt Nam, Bộ Thông tin và Truyền thông yêu cầu Quý cơ quan, tổ chức nghiêm túc, trách nhiệm chỉ đạo thực hiện:

1. Kiểm tra, rà soát và xác định các hệ thống thông tin có khả năng bị ảnh hưởng trong phạm vi quản lý của mình (đặc biệt lưu ý đối với các ứng dụng tự phát triển bằng Java). Thực hiện cập nhật bản vá bảo mật hoặc xử lý khắc phục theo khuyến nghị của nhà sản xuất. 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. Báo cáo về Bộ Thông tin và Truyền thông kết quả rà soát và xử lý khắc phục trước ngày 30/12/2021 để thực hiện tổng hợp báo cáo Thủ tướng Chính phủ. Báo cáo gửi trực tiếp về Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin qua thư điện tử: ais@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ Công an;
- Bộ Quốc phòng;
- Ban Cơ yếu Chính phủ;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Huy Dũng;
- Lưu: VT, Cục ATTT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Huy Dũng