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

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

Số: 8 /TTCNTT-KTHT
V/v ngăn chặn hoạt động tấn công mạng, khai thác lỗ hổng bảo mật trên Apache Log4j và Apache HTTP

Hà Nội, ngày 07 tháng 01 năm 2022

Kính gửi: Các đơn vị trực thuộc Bộ

Ngày 16/12/2021, Trung tâm Công nghệ thông tin (TTCNTT) gửi văn bản số 389/TTCNTT-KTHT cảnh báo về lỗ hổng trên Apache Log4j. Tiếp theo ngày 24/12/2021, TTCNTT tiếp tục gửi văn bản số 406/TTCNTT-KTHT yêu cầu các đơn vị rà soát, xử lý lỗ hổng này. Tuy nhiên, ngày 31/12/2021, Bộ Công an gửi Thông báo số 380/TB-BCA-A05 về việc ngăn chặn hoạt động tấn công mạng, khai thác lỗ hổng bảo mật trên Apache Log4j và Apache HTTP. Theo đó, Bộ Công an phát hiện hoạt động tấn công mạng, khai thác lỗ hổng bảo mật nhằm vào các máy chủ sử dụng Apache Log4j và Apache HTTP tại Việt Nam; nguy cơ lộ, mất thông tin bí mật, nhạy cảm, thông tin cá nhân của người dân Việt Nam, cụ thể như sau:

1. Lỗ hổng bảo mật trên Apache Log4j

Từ giữa tháng 12/2021, các chuyên gia công bố phát hiện 03 lỗ hổng bảo mật tồn tại trong Apache Log4j[1] phiên bản từ 2.0 đến 2.16, gồm: Log4Shell (CVE- 2021-44228), CVE-2021-45046 và CVE-2021-45105 cho phép tin tặc thực thi câu lệnh điều khiển từ xa, chiếm quyền quản trị, tấn công từ chối dịch vụ máy chủ web. Trong đó, lỗ hổng Log4Shell có mức độ nghiêm trọng cao nhất, đặc biệt nguy hiểm do việc khai thác đơn giản và đã bị công khai mã khai thác; nguy cơ ảnh hưởng tới hàng triệu trang web, hàng trăm sản phẩm của các hãng công nghệ trên thế giới[2] và Việt Nam. Mặc dù, cơ quan truyền thông, báo chí trong nước đã thông tin, cảnh báo rộng rãi nhưng nhiều cơ quan, tổ chức tại Việt Nam vẫn chưa thực hiện rà soát, khắc phục các lỗ hổng bảo mật.

Qua theo dõi, Bộ Công an phát hiện **hàng nghìn** sự kiện cảnh báo hoạt động tấn công mạng, khai thác lỗ hổng Log4Shell nhằm vào các cơ quan, tổ chức tại Việt Nam. Rà soát sơ bộ, Bộ Công an xác định ít nhất hàng trăm địa chỉ trang web thuộc quản lý của **43** cơ quan nhà nước, ngân hàng tại Việt Nam có nguy cơ bị ảnh hưởng bởi lỗ hổng Log4Shell. Đặc biệt nguy hiểm, các nhóm tin tặc nước ngoài đã tiến hành "vũ khí hóa" công cụ khai thác lỗ hổng Log4Shell, tích hợp các dòng mã độc có tính năng do thám, mã hóa dữ liệu; phát tán qua thư điện tử lừa đảo, thiết bị lưu trữ ngoài (USB, ổ đĩa xách tay) để xâm nhập, kiểm soát, tự động đánh cắp thông tin,

[1] Thư viện hỗ trợ việc ghi nhật ký hoạt động của máy chủ web sử dụng ngôn ngữ Java
[2] Bao gồm Microfocus, F5, Forescout, Fortinet, Amazon, Apple iCloud, Cisco, HPE, NVIDIA, Cloudflare, ElasticSearch, Imperva, NetApp, Neo4j, Nutanix, Oracle, Red Hat, Steam, Tesla, Twitter...

tài liệu trong hệ thống mạng; mã hóa dữ liệu để tống tiền; phá hủy cơ sở dữ liệu của các cơ quan, tổ chức.

2. Lỗ hổng bảo mật trên Apache HTTP

Ngày 20/12/2021, hãng bảo mật Sophos cảnh báo 02 lỗ hổng bảo mật nghiêm trọng (CVE-2021-44224, CVE-2021-44790) tồn tại trên Apache HTTP Server[3] phiên bản từ 2.4.51 trở xuống, cho phép tin tặc chiếm quyền quản trị từ xa máy chủ, kiểm soát, đánh cắp thông tin, dữ liệu hoặc thực hiện tấn công từ chối dịch vụ.

Qua theo dõi, Bộ Công an chưa ghi nhận hoạt động tấn công, khai thác 02 lỗ hổng trên vào các trang web thuộc quản lý của cơ quan nhà nước. Tuy nhiên, nhiều khả năng mã khai thác sẽ sớm được các đối tượng tin tặc, tội phạm mạng chia sẻ, rao bán để thực hiện tấn công mạng; nguy cơ ảnh hưởng tới **hàng trăm nghìn** máy chủ web của các cơ quan, tổ chức tại Việt Nam.

Từ tình hình trên, để tăng cường bảo đảm an ninh mạng, an toàn thông tin, TTCNTT đề nghị các Quý đơn vị nghiêm túc thực hiện:

(1) Chỉ đạo đơn vị chuyên trách tổ chức rà soát khắc phục lỗ hổng bảo mật tồn tại trong hệ thống mạng theo khuyến cáo của hãng phát triển, nhà sản xuất (*tham khảo Phụ lục 1);*

(2) Thiết lập, cập nhật dấu hiệu phát hiện, ngăn chặn hoạt động tấn công, khai thác lỗ hổng bảo mật, xâm nhập trái phép hệ thống mạng trên hệ thống giám sát, tường lửa, thiết bị phòng, chống tấn công mạng *(theo Phụ lục 2).*

Thông báo cho TTCNTT khi phát hiện dấu hiệu rà quét, khai thác lỗ hổng bảo mật từ địa chỉ IP Việt Nam vào hệ thống thông tin của Quý đơn vị, để kịp thời báo cáo, xử lý theo quy định của pháp luật.

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

[3] Apache HTTP Server là phần mềm dịch vụ máy chủ web phổ biến được sử dụng trên 31% số lượng trang web trên toàn thế giới

PHỤ LỤC 1
HƯỚNG DẪN RÀ SOÁT, KHẮC PHỤC LỖ HỔNG BẢO MẬT
(Kèm theo Công văn số 8 /TTCNTT-KTHT, ngày 07 /01 /2022 của Trung tâm Công nghệ thông tin)

I. Lỗ hổng bảo mật trên Apache Log4j

1. Rà soát, xác định nguy cơ

- Tra cứu, đối chiếu các sản phẩm, phần mềm đang sử dụng tại đơn vị với danh sách các phần mềm có nguy cơ tồn tại lỗ hổng bảo mật tại đường dẫn:

https://github.com/cisagov/log4j-affected-db/blob/develop/SOFTWARE-LIST.md

- Đối với các phần mềm dịch vụ do cơ quan tự xây dựng, phát triển, thực hiện tải xuống các công cụ rà quét lỗ hổng bảo mật Log4j tại đường dẫn: *https://github.com/CERTCC/CVE-2021-44228_scanner*. Sau đó, tiến hành khởi chạy câu lệnh kiểm tra trên máy chủ theo hệ điều hành tương ứng:

+ Đối với máy chủ Windows, sử dụng PowerShell chạy câu lệnh:

.\checkjndi.ps1 *[đường dẫn tới thư mục chứa thư viện log4j]*

+ Đối với máy chủ Linux, sử dụng terminal chạy câu lệnh:

bash ./checkjndi.sh *[đường dẫn tới thư mục chứa thư viện log4j]*

+ Hoặc, sử dụng công cụ được viết bằng Python trên cả 2 hệ điều hành có cài đặt Python 3 với câu lệnh:

python checkjndi.py *[đường dẫn tới thư mục chứa thư viện log4j]*

2. Khắc phục lỗ hổng bảo mật

- Cách ly vật lý hoặc logic máy chủ ứng dụng tồn tại lỗ hổng bảo mật.

- Cập nhật thư viện Apache Log4j trên máy chủ dịch vụ lên phiên bản 2.17.1 trở lên tại đường dẫn: *https://logging.apache.org/log4j/2.x/download.html*

- Trường hợp chưa thực hiện được việc nâng cấp bản vá:

(1) Cấu hình trong JVM args giá trị: *"-Dlog4j2.formatMsgNoLookups=true*";

(2) Cấu hình tường lửa các tập luật phát hiện tấn công thông qua tường lửa ứng dụng web (tham khảo *https://support.f5.com/csp/article/K19026212*); hạn chế tối đa các cổng kết nối mạng không cần thiết.

(3) Tăng cường giám sát, kiểm soát an ninh mạng.

II. Lỗ hổng bảo mật trên Apache HTTP

Tiến hành cập nhật phiên bản Apache HTTP Server 2.4.52 trên máy chủ dịch vụ theo hướng dẫn của nhóm phát triển tại đường dẫn:

https://downloads.apache.org/httpd/Announcement2.4.html

PHỤ LỤC 2
CÁC DẤU HIỆU NHẬN BIẾT, CẢNH BÁO (IOCs)
(Kèm theo Công văn số 8 /TTCNTT-KTHT, ngày 07 /01 /2022 của Trung tâm Công nghệ thông tin)

STT	IOCs	GHI CHÚ
1	apacheorg.xyz	Apache Log4j CnC
2	nazi.uy	Mirai Botnet
3	300gsyn.it	BillGates, Elknot Botnet
4	1cf9b0571decff5303ee9fe3c98bb1fl	Hash MD5
5	194db367fbb403a78d63818c3168a355	Hash MD5
6	18cc66e29a7bc435a316d9c292c45cc6	Hash MD5
7	1780d9aaf4c048ad99fa93b60777e3f9	Hash MD5
8	163e03b99c8cb2c71319a737932e9551	Hash MD5

PHỤ LỤC 3
DANH SÁCH CÁC HỆ THỐNG CỦA BỘ
CÓ NGUY CƠ BỊ ẢNH HƯỞNG BỞI LỖ HỔNG LOG4SHELL

(Kèm theo Công văn số 8 /TTCNTT-KTHT, ngày 07 /01 /2022 của Trung tâm Công nghệ thông tin)

STT	Tên miền
1	bcthanhtra.most.gov.vn
2	nextcloud.most.gov.vn
3	motcuabkhcn.most.gov.vn
4	vistip.most.gov.vn
5	tthc.most.gov.vn
6	iprenforcement.most.gov.vn
7	b.vjst.vn

DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN

(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2022 của Trung tâm Công nghệ thông tin)

TT	Tên đơn vị
1.	Thanh tra Bộ
2.	Cục Công tác phía Nam
3.	Cục Ứng dụng và phát triển công nghệ
4.	Cục Năng lượng nguyên tử
5.	Cục Thông tin Khoa học và Công nghệ Quốc gia
6.	Cục Phát triển thị trường và doanh nghiệp khoa học và công nghệ
7.	Cục An toàn bức xạ và hạt nhân
8.	Cục Sở hữu trí tuệ
9.	Tổng Cục tiêu chuẩn đo lường chất lượng
10.	Ban quản lý khu công nghệ cao Hoà Lạc
11.	Học viện Khoa học, Công nghệ và Đổi mới sáng tạo
12.	Viện Khoa học và công nghệ Việt Nam - Hàn Quốc (VKIST)
13.	Viện Nghiên cứu sáng chế và Khai thác công nghệ
14.	Viện Năng lượng nguyên tử Việt Nam
15.	Viện Ứng dụng công nghệ
16.	Viện Đánh giá khoa học và Định giá công nghệ
17.	Viện Khoa học sở hữu trí tuệ
18.	Viện Nghiên cứu và Phát triển Vùng
19.	Văn phòng các Chương trình trọng điểm cấp nhà nước
20.	Văn phòng Công nhận chất lượng
21.	Văn phòng Đăng ký hoạt động khoa học và công nghệ
22.	Văn phòng các Chương trình khoa học và công nghệ quốc gia
23.	Báo Khoa học và Phát triển
24.	Tạp chí Khoa học và Công nghệ Việt Nam
25.	Nhà xuất bản Khoa học và Kỹ thuật
26.	Quỹ Phát triển khoa học và công nghệ quốc gia
27.	Quỹ Đổi mới công nghệ quốc gia
28.	Trung tâm Nghiên cứu và Phát triển truyền thông khoa học và công nghệ
29.	Trung tâm Nghiên cứu và Phát triển hội nhập khoa học và công nghệ quốc tế
30.	Báo điện tử Tin nhanh Việt Nam (VnExpress)