Ký bởi Administrator
Giờ ký: 2022-01-17T09:20:27.0147625+07:00

ỦY BAN NHÂN DÂN QUẬN BA ĐÌNH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 90 /UBND-VP V/v ngăn chặn hoạt động tấn công mạng, khai thác lỗ hổng bảo mật trên Apache Log4j và Apache HTTP	*Ba Đình, ngày 14 tháng 01 năm 2022.*

Kính gửi:

- Trưởng Công an quận; Trưởng phòng GD và ĐT;
- Thủ trưởng các đơn vị sự nghiệp, hiệp quản trên địa bàn quận;
- Hiệu trưởng các trường Mầm non, Tiểu học, THCS.

Thực hiện chỉ đạo của UBND Thành phố tại văn bản số 89/UBND-NC ngày 11/01/2022 và Thông báo số 380/TB-BCA-A05 ngày 31/12/2021 của Bộ Công an *(có bản chụp gửi kèm)* về ngăn chặn hoạt động tấn công mạng, khai thác lỗ hổng bảo mật Apache Log4j và Apache HTTP trên các website, phần mềm sử dụng máy chủ Web Server Apache. Ủy ban nhân dân quận yêu cầu:

1. Đề nghị Thủ trưởng các cơ quan, đơn vị và Hiệu trưởng các trường Mầm non, Tiểu học, THCS căn cứ nội dung chỉ đạo của UBND Thành phố và thông báo của Bộ Công an, triển khai rà soát các website, các phần mềm sử dụng mã nguồn mở như: PHP, Python, Perl… và máy chủ Webserver Apache tại đơn vị mình, chủ động liên hệ với đơn vị cung cấp dịch vụ website, dịch vụ máy chủ để khắc phục các lỗ hổng bảo mật đã được Bộ Công an cảnh báo. Nếu có khó khăn, vướng mắc kịp thời liên hệ với cơ quan an ninh mạng thuộc Công an Thành phố, Sở Thông tin và Truyền thông để xem xét, giải quyết.

2. Giao Công an quận chủ trì, phối hợp với Phòng Văn hóa và Thông tin bám sát chỉ đạo của Công an Thành phố, Sở Thông tin và Truyền thông hướng dẫn các cơ quan, đơn vị và các trường Mầm non, Tiểu học, THCS thực hiện nội dung trên.

UBND quận yêu cầu Thủ trưởng các cơ quan, đơn vị nghiêm túc thực hiện./.

Nơi nhận:
- Như trên;
- UBND Thành phố;
- Đ/c Lê Hồng Sơn - PCT TT UBND Thành phố;
- Công an Thành phố;
- TT Quận ủy, TT HĐND quận;
- Đ/c Chủ tịch, các đ/c PCT UBND quận;
- VPUB: CVP, Tổ CV Tổng hợp, CV CNTT;
- Lưu VT.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Tạ Nam Chiến

Nhân dân Thành phố
Ngày ký: 11/01/2022
09:38:35 +07:00

VĂN PHÒNG

ỦY BAN NHÂN DÂN **THÀNH PHỐ HÀ NỘI**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 89 /UBND – NC V/v ngăn chặn hoạt động tấn công mạng, khai thác lỗ hổng bảo mật trên Apache Log4j và Apache HTTP	*Hà Nội, ngày 11 tháng 01 năm 2022*

Kính gửi:
- Các Sở, ban, ngành Thành phố;
- UBND các quận, huyện, thị xã.

Thực hiện Thông báo số 380/TB-BCA-A05 ngày 31/12/2021 của Bộ Công an về việc "ngăn chặn hoạt động tấn công mạng, khai thác lỗ hổng bảo mật trên Apache Log4j và Apache HTTP" *(bản chụp kèm theo)*, UBND Thành phố chỉ đạo như sau:

- Yêu cầu các Sở, ban, ngành Thành phố, UBND các quận, huện, thị xã căn cứ nội dung Thông báo nêu trên của Bộ Công an, triển khai thực hiện tại đơn vị mình, chủ động liên hệ với Công an Thành phố, Sở Thông tin và Truyền thông để được hướng dẫn triển khai thực hiện *(trường hợp có khó khăn, vướng mắc)*.

- Giao Công an Thành phố chủ trì phối hợp với Sở Thông tin và Truyền thông theo chức năng, nhiệm vụ được giao, hướng dẫn các đơn vị triển khai thực hiện trên địa bàn thành phố, tổng hợp, báo cáo cấp có thẩm quyền theo quy định./.

Nơi nhận:
- Như trên;
- Bộ Công an;
- Thường trực Thành ủy;
- Chủ tịch UBND Thành phố;
- PCT TTUBND TP Lê Hồng Sơn;
- VPUB: CVP, PCVP V.T.Anh, NC(Trung), TTTH&CB;
- Lưu: VT. (SĐ: 161)

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Lê Hồng Sơn

BỘ CÔNG AN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
Số: 380/TB-BCA-A05	*Hà Nội, ngày 31 tháng 12 năm 2021*

VĂN PHÒNG UBND TP. HÀ NỘI
ĐẾN Số: 167
Ngày 05/1
Chuyển: ..an phát hiện hoạt động tấn công mạng, khai thác lỗ hổng bảo mật
Lưu hồ sơ

THÔNG BÁO

V/v ngăn chặn hoạt động tấn công mạng, khai thác lỗ hổng bảo mật trên Apache Log4j và Apache HTTP

Qua công tác bảo đảm an ninh hệ thống mạng thông tin quốc gia, 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. Bộ Công an thông báo về các lỗ hổng bảo mật 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 (*gửi kèm riêng theo từng đơn vị có liên quan*). 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, 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-202144790) tồn tại trên Apache HTTP Server[3]

---

[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...

[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

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.

3. Từ tình hình trên, để tăng cường bảo đảm an ninh mạng, an toàn thông tin, Bộ Công an đề nghị các bộ, ban, ngành, địa phương, tập đoàn, tổng công ty thuộc quản lý của nhà nước; các ngân hàng; các đơn vị cung cấp dịch vụ Internet tại Việt Nam:

(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 hướng dẫn kèm theo*);

(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 (*có danh sách đính kèm*).

Thông báo cho Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an, địa chỉ: *207 Khuất Duy Tiến, Nhân Chính, Thanh Xuân, Hà Nội* 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 cơ quan, tổ chức trong nước để kịp thời đấu tranh, xử lý theo quy định của pháp luật.

Bộ Công an xin thông báo./.

Nơi nhận:
- Đ/c Bộ trưởng Tô Lâm
- Các đồng chí Thứ trưởng

(để báo cáo);

- Văn phòng TW Đảng
- Văn phòng Tổng Bí thư
- Văn phòng Chủ tịch nước
- Văn phòng Quốc hội
- Văn phòng Chính phủ
- Các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ
- Tỉnh ủy, Thành ủy, UBND các tỉnh, TP trực thuộc TW
- Tòa án nhân dân tối cao
- Viện kiểm sát nhân dân tối cao
- Kiểm toán nhà nước
- Các tập đoàn, tổng công ty: EVN, PVN, VNA, VATM, ACV
- Các ngân hàng: BIDV, Agribank, Vietinbank, Vietcombank

(để phối hợp);

- Các đơn vị cung cấp dịch vụ Intenet
- Công an các đơn vị, địa phương

(để thực hiện);

- Lưu: VT, A05(P8).

TUQ. BỘ TRƯỞNG
CỤC TRƯỞNG CỤC AN NINH MẠNG VÀ PCTP SỬ DỤNG CÔNG NGHỆ CAO

Trung tướng Nguyễn Minh Chính

PHỤ LỤC 1
HƯỚNG DẪN RÀ SOÁT, KHẮC PHỤC LỖ HỔNG BẢO MẬT
(Kèm theo Thông báo số 380/TB-BCA-A05, ngày 31/12/2021)

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 sbản 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/Anouncement2.4.html

PHỤ LỤC 2
CÁC DẤU HIỆU NHẬN BIẾT, CẢNH BÁO (IOCs)
(Kèm theo Thông báo số 380/TB-BCA-A05, ngày 31/12/2021)

STT	IOCs	GHI CHÚ
1	apacheorg.xyz	Apache Log4j CnC
2	nazi.uy	Mirai Botnet
3	300gsyn.it	BillGates, Elknot Botnet
4	1cf9b0571decff5303ee9fe3c98bb1f1	Hash MD5
5	194db367fbb403a78d63818c3168a355	Hash MD5
6	18cc66e29a7bc435a316d9c292c45cc6	Hash MD5
7	1780d9aaf4c048ad99fa93b60777e3f9	Hash MD5
8	163e03b99c8cb2c71319a737932e9551	Hash MD5