BỘ CÔNG AN
CÔNG AN TỈNH NGHỆ AN

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

Số: 1198/CAT-PA05
V/v rà soát khắc phục điểm yếu hệ thống thông tin

Nghệ An, ngày 21 tháng 3 năm 2025

Kính gửi: UBND tỉnh Nghệ An

Qua công tác trinh sát, nắm tình hình, rà soát, bảo đảm an toàn, an ninh mạng đối với các hệ thống thông tin thuộc Đề án 06, Bộ Công an đã phát hiện điểm yếu trong việc thiết lập cấu hình trên thiết bị cân bằng tải F5 Big-IP gây nguy cơ lộ lọt cấu trúc mạng bên trong hệ thống thông tin. Vấn đề này là điểm yếu có thể bị lợi dụng trong các cuộc tấn công mạng vào hệ thống, cụ thể như sau:

Khi một người dùng internet truy cập vào Hệ thống thông tin giải quyết thủ tục hành chính của tỉnh A, thiết bị cân bằng tải thực hiện điều hướng yêu cầu truy cập vào một máy chủ ứng dụng bên trong hệ thống và giữ phiên truy cập của người dùng đó với máy chủ ứng dụng thông qua giá trị cookies trên trình duyệt web do thiết bị cân bằng tải tạo ra. Nếu giá trị cookies này được thiết lập tạo theo cơ chế mặc định thì dễ dàng giải mã theo nguyên tắc tạo của hãng sản xuất thiết bị cân bằng tải. Khi đó sẽ để lộ 02 thông tin nhạy cảm, gồm: tên thiết bị giải pháp cân bằng tải và địa chỉ IP, cổng kết nối của máy tính với máy chủ ứng dụng nội bộ bên trong hệ thống.

Vậy, Công an tỉnh Nghệ An kính báo cáo, đề xuất UBND tỉnh chỉ đạo các Sở, Ban, Ngành, UBND các cấp tổ chức rà soát, khắc phục (nếu có) đối với hệ thống thông tin thuộc hệ thống dịch vụ công trực tuyến *(kèm theo Hướng dẫn khai thác và khắc phục)*.

Công an tỉnh Nghệ An phân công đ/c Trung tá Võ Thanh Liêm – cán bộ Phòng PA05 *(SĐT: 0977499007)* làm đầu mối phụ trách hướng dẫn./.

Nơi nhận:
- Đ/c Giám đốc CAT *(để báo cáo);*
- Như trên *(để thực hiện);*
- Lưu: VT CAT, PA05(VTL).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

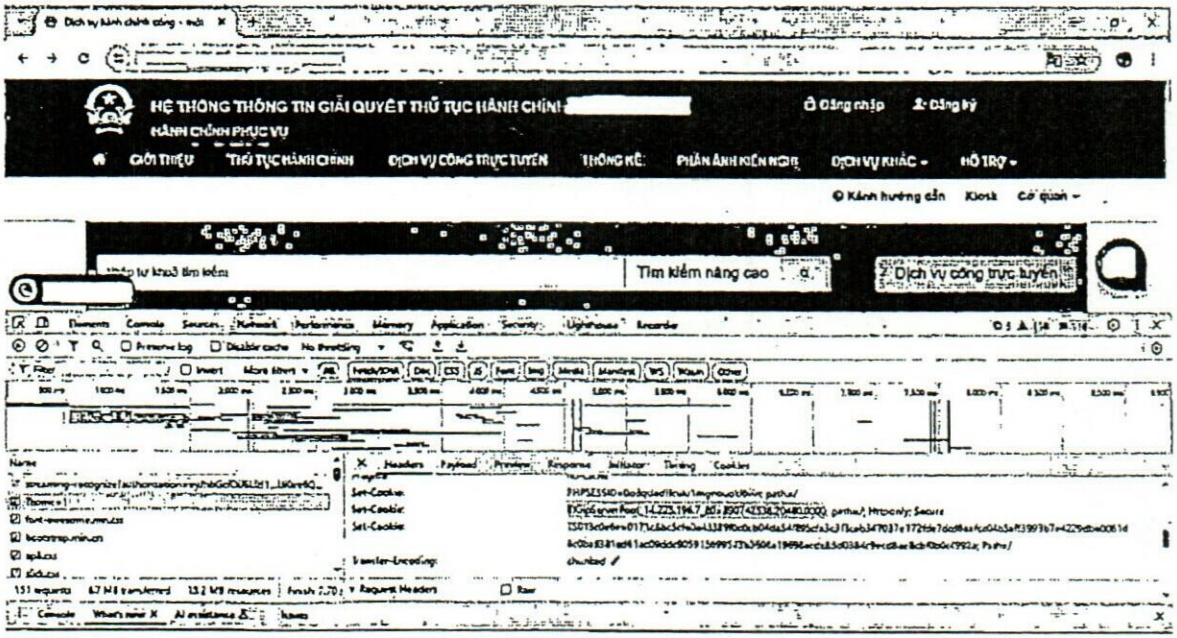
Đại tá Lê Văn Thái

PHỤ LỤC
HƯỚNG DẪN KHAI THÁC VÀ KHẮC PHỤC ĐIỂM YẾU BẢO MẬT

Quy trình phát hiện và giải mã thu thập thông tin địa chỉ IP nội bộ:

Bước 1: Khởi động trình duyệt, bật tính năng developer Tools bằng cách nhấn phím F12, chọn thẻ "Network" trên trình duyệt.

Bước 2: Truy cập trang web cần kiểm tra, tìm thông tin cookies trong Request Header. Nhận biết điểm yếu bảo mật nếu có tiền tố BIGipServer (thiết bị F5 Big-IP) và giá trị cookies có cấu trúc dạng 890742538.20480.0000 (địa chỉ IP private, Cổng kết nối tới máy chủ bên trong).



Thông tin cookies của hệ thống thông tin giải quyết thủ tục hành chính

Bước 3: Thu thập, phân tích thông tin từ cookies

BIGipServerPool_14.225.196.7_80=890742538.20480.0000

- Tham số BIGipServerPool_14.225.196.7_80 có cấu trúc BIGipServer_PoolName. Hiện tại đối với hệ thống này, PoolName sử dụng địa chỉ IP public (14.225.196.7) của hệ thống.

- Tham số 890742538.20480.0000 có cấu trúc IPprivate.Port.0000 thể hiện máy chủ ứng dụng bên trong hệ thống xử lý các truy vấn của người dùng (vùng mạng máy chủ ứng dụng nội bộ). Thực hiện giải mã tham số này:

+ Giá trị địa chỉ IP dạng thập phân **890742538**, chuyển đổi sang Hex được 3517A70A tương đương giá trị địa chỉ IP dạng hex 35.17.A7.0A, đảo

ngược địa chỉ IP dạng hex nhận được 0A.A7.17.35, đổi sang dạng thập phân sẽ nhận được địa chỉ IP nội bộ **10.167.23.53** (đây là nguyên tắc tạo giá trị cookies mặc định của F5).

+ Giá trị cổng kết nối dạng thập phân **20480**, tính toán theo nguyên tắc tạo cookies của F5 sẽ nhận được giá trị cổng **80.**

Bước 4: Phương án khắc phục

- Tắt giá trị cookies này nếu không cần thiết;

- Nếu sử dụng thì thay đổi tiền tố BIGipServer (không để mặc định) và sử dụng thuật toán mã hóa giá trị cookies được tích hợp sẵn trong thiết bị F5.