UBND TỈNH THÁI NGUYÊN **SỞ VĂN HÓA, THỂ THAO VÀ DU LỊCH**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 3657 /SVHTTDL-TCHC V/v cảnh báo lỗ hổng an toàn thông tin trong sản phẩm BIG-IP	*Thái Nguyên, ngày 06 tháng 11 năm 2023*

Kính gửi:
- Các phòng thuộc Sở;
- Các đơn vị sự nghiệp trực thuộc Sở.

Sở Văn hóa, Thể thao và Du lịch nhận được Công văn số 2935/STTTT-CNTT, ngày 03/11/2023 của Sở Thông tin và Truyền thông về việc cảnh báo lỗ hổng an toàn thông tin trong sản phẩm BIG-IP.

Để đảm bảo an toàn thông tin cho hệ thống thông tin của cơ quan, đơn vị, góp phần đảm bảo an toàn cho các hệ thống thông tin dùng chung, liên thông của tỉnh, Sở Văn hóa, Thể thao và Du lịch gửi các phòng thuộc Sở, các đơn vị sự nghiệp thuộc Sở thông tin về lỗ hổng an toàn thông tin có mức độ ảnh hưởng nghiêm trọng trong các thiết bị cân bằng tải F5 BIG-IP và biện pháp khắc phục do Sở Thông tin và Truyền thông cung cấp và hướng dẫn.

(*Chi tiết tại Phụ lục gửi kèm theo*)

Sở Văn hóa, Thể thao và Du lịch yêu cầu các phòng, đơn vị triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Sở Thông tin và Truyền thông;
- Lãnh đạo Sở;
- Lưu: VT, TCHC. (Thoa01b)

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ VĂN HÓA THỂ THAO VÀ DU LỊCH
TỈNH THÁI NGUYÊN

Lê Ngọc Linh

PHỤ LỤC: THÔNG TIN LỖ HỔNG AN TOÀN THÔNG TIN

(Kèm theo Công văn số /STTTT-CNTT ngày / /2023 của Sở Thông tin và Truyền thông)

1. Thông tin lỗ hổng an toàn thông tin

- Mô tả lỗ hổng bảo mật: CVE-2023-46747.

Đây là lỗ hổng mới nhất được công bố sau bản vá đặc biệt (hotfix) trên Thiết bị cân bằng tải F5 BIG-IP của Công ty F5 Networks và có liên quan chặt chẽ tới lỗ hổng CVE-2022-26377. Lỗ hổng mới xảy ra do lỗi Request Smuggling trong Apache JServ Protocol (AJP) được sử dụng bởi các thiết bị của hãng. Đối tượng tấn công có thể khai thác lỗ hổng này để vượt qua cơ chế xác thực và lạm dụng tính năng Traffic Management User Interface (TMUI) nhằm thực thi mã từ xa. Thông tin kỹ thuật của lỗ hổng đã được một số nhà nghiên cứu bảo mật công bố.

- Mức độ ảnh hưởng: Được đánh giá có mức độ ảnh hưởng nghiêm trọng (với điểm đánh giá CVSS là 9.8/10).

- Phiên bản bị anh hưởng: Lỗ hổng này ảnh hưởng đến tất cả các phiên bản F5 BIG-IP; từ phiên bản 13.1.0 đến 13.1.5, từ 14.1.0 đến 14.1.5, từ 15.1.0 đến 15.1.10, từ 16.1.0 đến 16.1.4 và 17.1.0.

2. Hướng dẫn khắc phục

- Nhằm đảm bảo an toàn hệ thống, đề nghị bộ phận chuyên trách về công nghệ thông tin/an toàn thông tin tại các cơ quan, đơn vị kiểm tra, rà soát tại đơn vị có đang sử dụng các Thiết bị cân bằng tải F5 BIG-IP của Công ty F5 Networks. Trong trường hợp đang sử dụng các Thiết bị cân bằng tải F5 BIG-IP có khả năng bị ảnh hưởng bởi lỗ hổng trên, thực hiện nâng cấp lên phiên bản mới nhất để tránh nguy cơ bị tấn công; trong trường hợp chưa thể nâng cấp cần thực hiện làm theo hướng dẫn của hãng (*Tham khảo thông tin tại địa chỉ: https://my.f5.com/manage/s/article/K000137353).*

- 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 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.

- Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ:

+ Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: nscs@ais.gov.vn.

+ Sở Thông tin và Truyền thông: ông Nguyễn Quang Huy, Chuyên viên phòng Công nghệ thông tin, số điện thoại: 0915.373.585.

+ Đội Ứng cứu sự cố An toàn thông tin trong các cơ quan nhà nước tỉnh Thái Nguyên: Ông Tạ Tuấn Dũng, Trưởng phòng Quản trị hệ thống và An ninh mạng, Trung tâm Công nghệ thông tin và Truyền thông, Đội phó Đội Ứng cứu sự cố, điện thoại: 0914.300.486.