UBND TỈNH TÂY NINH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 2180 /STTTT-TTGSĐH
V/v cảnh báo lỗ hổng an toàn thông tin ảnh hưởng nghiêm trọng trong F5 BIG-IP

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

Tây Ninh, ngày24 tháng 11 năm 2023

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các cơ quan tham mưu, giúp việc Tỉnh ủy;
- Mặt trận Tổ quốc và các Đoàn thể chính trị - xã hội;
- Các Sở, ban, ngành tỉnh;
- Các đơn vị ngành dọc;
- Các huyện, thị, thành ủy trực thuộc Tỉnh ủy;
- UBND các huyện, thị xã, thành phố;
- UBND các xã, phường, thị trấn.

Thực hiện theo Công văn số 1943/CATTT-NCSC của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc cảnh báo lỗ hổng an toàn thông tin ảnh hưởng nghiêm trọng trong F5 BIG-IP ***(Thông tin chi tiết phụ lục kèm theo)***.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các đơn vị và góp phần đảm bảo an toàn thông tin trên địa bàn tỉnh, Sở Thông tin và Truyền thông đề nghị các đơn vị, địa phương thực hiện gấp các công việc cụ thể như sau:

1. Kiểm tra, rà soát các sản phẩm F5 BIG-IP đang sử dụng 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 F5.

2. 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 uy tín về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

Thông tin liên quan đề nghị liên hệ Ông Vương Duy Thanh - Trung tâm Giám sát, điều hành kinh tế, xã hội tập trung; Điện thoại: 0932624462.

Trân trọng./.

Nơi nhận:
- Như trên;
- BGĐ Sở (b/c);
- P.CNTTBCVT;
- Lưu: VT, TTGSĐH.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH TÂY NINH

Nguyễn Trung Hiếu

PHỤ LỤC
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT

1.Thông tin lỗ hổng bảo mật

- Mô tả:

- CVE-2023-46747 được đánh giá ở mức độ Nghiêm trọng (Điểm CVSS: 9.8) là lỗ hổng mới nhất được công bố sau bản vá đặc biệt (hotfix) của F5 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.

- **Ảnh hưởng:** F5 BIG-IP (all modules) phiên bản từ 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.

- **Đánh giá mức độ:** Đánh giá sơ bộ từ các chuyên gia bảo mật, lỗ hổng này ảnh hưởng đến nhiều thiết bị trên toàn cầu trong đó có cả Việt Nam. Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) đánh giá khả năng các mã khai thác của các lỗ hổng này sẽ sớm được công khai trên Internet trong thời gian sắp tới.

2. Hướng dẫn khắc phục:

Biện pháp tốt nhất để khắc phục lỗ hổng bảo mật nói trên là cập nhật lên phiên bản mới. Trong trường hợp chưa thể nâng cấp, Quý đơn vị cần thực hiện theo hướng dẫn của hãng F5 (*https://my.f5.com/manage/s/article/K000137353*).

1. Nguồn tham khảo:

https://my.f5.com/manage/s/article/K000137353