BỘ THÔNG TIN TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

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

Số: 1943 /CATTT-NCSC
V/v lỗ hổng an toàn thông tin ảnh hưởng nghiêm trọng trong F5 BIG-IP

Hà Nội, ngày 01 tháng 11 năm 2023

Kính gửi:

- Đơn vị chuyên trách về CNTT các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước; các Ngân hàng TMCP; các tổ chức tài chính;
- Hệ thống các đơn vị chuyên trách về an toàn thông tin.

Qua công tác giám sát an toàn thông tin trên không gian mạng, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin, ghi nhận mã khai thác của lỗ hổng CVE-2023-46747 cho phép đối tượng tấn công vượt qua cơ chế xác thực và lạm dụng tính năng Traffic Management User Interface (TMUI) nhằm thực thi mã từ xa. Lỗ hổng CVE-2023-46747 được đánh giá ở mức độ Nghiêm trọng, việc rà soát và nâng cấp phiên bản hoặc áp dụng biện pháp khắc phục thay thế cần được thực hiện ngay lập tức.

Thông tin chi tiết lỗ hổng bảo mật có tại phụ lục kèm theo.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Cục An toàn thông tin khuyến nghị Quý đơn vị thực hiện:

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. *(Tham khảo thông tin tại phụ lục kèm theo).*

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.

3. Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của 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.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Huy Dũng (để b/c);
- Cục A05, Bộ Công an;
- Bộ Tư lệnh 86, Bộ Quốc phòng;
- Ban Cơ yếu Chính phủ;
- Đơn vị chuyên trách về ATTT/CNTT của: Văn phòng TW Đảng; Văn phòng Quốc hội; Văn phòng Chủ tịch nước; Kiểm toán Nhà nước; Viện Kiểm sát nhân dân tối cao; Tòa án nhân dân tối cao;
- Cục trưởng (để b/c);
- Các Phó Cục trưởng;
- Trung tâm VNCERT/CC, Phòng ATHTTT;
- Lưu: VT, NCSC.LTQ.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Trần Đăng Khoa

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT
(Kèm theo Công văn số /CATTT-NCSC ngày / /2023 của Cục An toàn thông tin)

1. Thông tin các 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.

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*).

3. Tài liệu tham khảo

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