BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

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

Số: /CATTT-NCSC
V/v nguy cơ tấn công vào hệ thống thông tin của các cơ quan, tổ chức sử dụng thiết bị F5 BIG-IP

Hà Nội, ngày tháng năm

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.

Thực hiện chức năng, nhiệm vụ được giao, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin thường xuyên thực hiện công tác theo dõi, giám sát trên không gian mạng nhằm phát hiện và ngăn chặn sớm các nguy cơ gây mất an toàn thông tin.

Qua công tác theo dõi thông tin trên không gian mạng và hoạt động hợp tác, chia sẻ thông tin với các tổ chức lớn về an toàn thông tin trong và ngoài nước, Cục An toàn thông tin phát hiện hiện nhiều hệ thống thông tin sử dụng thiết bị F5 có khả năng bị tấn công thông qua lỗ hổng trong thiết bị F5 BIG-IP Traffic Management User Interface (TMUI) (**CVE-2020-5902**). Những lỗ hổng này ảnh hưởng các phiên bản của BIG-IP từ 11.x đến 15.x cho phép đối tượng tấn công chèn và thực thi mã từ xa, chiếm quyền kiểm soát hệ thống.

Đây là lỗ hổng bảo mật đặc biệt nghiêm trọng (CVSS = 10.0), được phát hiện trong giao diện người dùng quản lý lưu lượng truy cập của thiết bị BIG-IP. Khai thác thành công lỗ hổng này, đối tượng tấn công có thể thu thập thông tin, có khả năng tạo hoặc xóa tệp, vô hiệu hóa các dịch vụ, chạy các lệnh hệ thống với mã Java tùy ý, chiếm quyền kiểm soát hệ thống mục tiêu.

Theo thống kê tính đến tháng 6 năm 2020, có hơn 8,000 thiết bị trên Internet đang có nguy cơ bị tấn công bởi lỗ hổng bảo mật này. Qua đánh giá sơ bộ của Trung tâm NCSC, Việt Nam có hàng trăm hệ thống đang sử dụng thiết bị F5 BIG-IP. Đây là những hệ thống đầu tiên nằm trong mục tiêu mà đối tượng tấn công sẽ tìm đến.

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 đề nghị Quý đơn vị thực hiện:

1. Kiểm tra, rà soát hệ thống thông tin có khả năng bị ảnh hưởng bởi lỗ hổng trên và có phương án xử lý, khắc phục lỗ hổng.

2. Rà soát lại toàn bộ hệ thống thông tin của Quý đơn vị, thường xuyên kiểm tra, đánh giá để chủ động phát hiện và xử lý kịp thời các lỗ hổng bảo mật.

3. Tăng cường theo dõi giám sát hệ thống đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn để phát hiện kịp thời các nguy cơ tấn công mạng.

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 0243.209.1616, thư điện tử: ais@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Thành Hưng (để b/c);
- Cục trưởng (để b/c);
- PCT Nguyễn Khắc Lịch;
- Lưu: VT, NCSC.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

Nguyễn Khắc Lịch

Phụ lục
Danh sách các sản phẩm bị ảnh hưởng
(Kèm theo Công văn số /CATTT-NCSC ngày / / 2020)

Sản phẩm		Phiên bản bị ảnh hưởng	Phiên bản cập nhật bản vá
BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, FPS, GTM, Link Controller, PEM)	15.x	15.1.0	15.1.0.4
		15.0.0	
	14.x	14.1.0 - 14.1.2	14.1.2.6
	13.x	13.1.0 - 13.1.3	13.1.3.4
	12.x	12.1.0 - 12.1.5	12.1.5.2
	11.x	11.6.1 - 11.6.5	11.6.5.2