UBND TỈNH ĐỒNG NAI
SỞ Y TẾ

Số: 3856 /SYT-VP
V/v triển khai Công văn số 1857/STTTT-CNTTVT ngày 10/7/2020 của Sở Thông tin và Truyền thông.

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

Đồng Nai, ngày 15 tháng 7 năm 2020

Kính gửi: Giám đốc, Thủ trưởng các đơn vị trực thuộc.

Sở Y tế Đồng Nai nhận được Công văn số 1857/STTTT-CNTTVT ngày 10/7/2020 của Sở Thông tin và Truyền thông về việc nguy cơ tấn công vào hệ thống thông tin của các cơ quan, tổ chức sử dụng thiết bị F5 BIG-IP (*Đính kèm Công văn*).

Giám đốc Sở Y tế đề nghị Giám đốc, Thủ trưởng các đơn vị trực thuộc chỉ đạo các tổ chức, cá nhân phụ trách về công nghệ thông tin của đơn vị tổ chức triển khai thực hiện nội dung Công văn số 1857/STTTT-CNTTVT ngày 10/7/2020 của Sở Thông tin và Truyền thông.

Đề nghị Giám đốc, Thủ trưởng các đơn vị trực thuộc triển khai thực hiện theo sự chỉ đạo./.

Nơi nhận:
- Như trên;
- Lưu: VT,VP.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Nguyễn Hữu Tài

Số 2 - Phan Đình Phùng, phường Quang Vinh, thành phố Biên Hoà, tỉnh Đồng Nai
ĐT: (02513) 942641, Fax: (02513) 847269, Email: syt@dongnai.gov.vn, Website: syt.dongnai.gov.vn

UBND TỈNH ĐỒNG NAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 1857 /STTTT-CNTTVT
V/v nguy cơ tấn công vào hệ thống thông tin của các cơ quan, tổ chức sử dụng thiết bị F5 BIG-IP

Đồng Nai, ngày 10 tháng 7 năm 2020

Kính gửi:
- Các cơ quan Đảng, Nhà nước và các đoàn thể trên địa bàn tỉnh;
- Viettel Chi nhánh Đồng Nai, VNPT Đồng Nai;
- Trung tâm Công nghệ thông tin và Truyền thông.

Ngày 07/7/2020, Cục An toàn thông tin có văn bản số 564/CATTT-NCSC về việc nguy cơ tấn công vào hệ thống thông tin của các cơ quan, tổ chức sử dụng thiết bị F5 BIG-IP. Theo đó, Cục An toàn thông tin đã phát 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 Giám sát an toàn không gian mạng quốc gia (Trung tâm NCSC) – thuộc Cục An toàn thông tin, Việt Nam có hàng trăm hệ thống đang sử dụng thiết bị F5 BIGIP. Đây là những hệ thống đầu tiên nằm trong mục tiêu mà đối tượng tấn công sẽ tìm đến.

Để tăng cường đảm bảo an toàn thông tin mạng trên địa bàn tỉnh, Sở Thông tin và Truyền thông đề nghị Quý đơn vị chủ động thực hiện các biện pháp sau:

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) hoặc Sở Thông tin và Truyền thông, điện thoại 0251.3810.269, thư điện tử: attt@dongnai.gov.vn./.

Trân trọng./.

Đính kèm: Danh sách các sản phẩm bị ảnh hưởng.

Nơi nhận:
- Như trên;
- UBND tỉnh (b/c);
- Giám đốc và Phó Giám đốc Sở;
- Lưu: VT, CNTTVT, Thịnh.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH ĐỒNG NAI

Võ Hoàng Khai

Phụ lục

Danh sách các sản phẩm bị ảnh hưởng

(Kèm theo văn bản số /STTTT-CNTTVT ngày /7/2020)

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

Phụ lục

DANH SÁCH CÁC SẢN PHẨM BỊ ẢNH HƯỞNG

(Kèm theo văn bản số /STTTT-CNTTVT ngày /7/ 2020 của Sở Thông tin và Truyền thông)

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