UBND TỈNH NAM ĐỊNH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số:988 /STTTT-CĐS
V/v kiểm tra, rà soát và khắc phục lỗ hổng bảo mật ảnh hưởng nghiêm trọng trong F5 BIG-IP

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

Nam Định, ngày 07 tháng 11 năm 2023

Kính gửi:
- Các sở, ban, ngành của tỉnh;
- UBND các huyện, thành phố;
- VNPT Nam Định;
- Viettel Nam Định.

Căn cứ Văn bản số 1943/CATTT-NCSC ngày 01/11/2023 của Cục An toàn thông tin về việc cảnh báo lỗ hổng bảo mật ảnh hưởng nghiêm trọng trong các sản phẩm cân bằng tải F5 BIG-IP của hãng F5 Networks (*có trụ sở tại Washington, Mỹ*).

Theo đó, 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 các lỗ hổng bảo mật có tại phụ lục kèm theo.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan, doanh nghiệp trên địa bàn tỉnh, Sở Thông tin và Truyền thông đề nghị các sở, ban, ngành của tỉnh; UBND các huyện, thành phố và VNPT Nam Định, Viettel Nam Định phối hợp triển khai thực hiện một số nội dung sau:

1. Kiểm tra, rà soát các sản phẩm F5 BIG-IP (nếu 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 kịp thời thông báo về Sở Thông tin và Truyền thông khi phát hiện có dấu hiệu bị khai thác, tấn công mạng.

3. Yêu cầu Trung tâm Chuyển đổi số và Truyền thông:

- Thực hiện rà soát, kiểm tra, cập nhật bản vá bảo mật cho thiết bị F5 BIG-IP tại Trung tâm Tích hợp dữ liệu của tỉnh.

- Làm đầu mối hỗ trợ, hướng dẫn các sở, ban, ngành của tỉnh; UBND các huyện, thành phố xử lý, khắc phục lỗ hổng.

Sở Thông tin và Truyền thông đề nghị các Sở, ban, ngành của tỉnh; UBND các huyện, thành phố và VNPT Nam Định, Viettel Nam Định quan tâm phối hợp triển khai thực hiện.

Thông tin liên hệ: Đầu mối hỗ trợ kỹ thuật: ông Trần Tuấn Anh, Kỹ sư Trung tâm Chuyển đổi số và Truyền thông (số điện thoại: 0376805976, email: trantuananh.stt@namdinh.gov.vn); Đầu mối tổng hợp: ông Phạm Văn An, Chuyên viên Phòng Chuyển đổi số (điện thoại: 0949268749, email: phamvanan.stt@namdinh.gov.vn).

Trân trọng./.

Nơi nhận:
- Như trên;
- Phòng VHTT các huyện, TP;
- Trung tâm VHTT&TT các huyện, TP;
- Trung tâm CĐS&TT (để thực hiện);
- Cổng TTĐT;
- Lưu: VT, CĐS (anpv).

GIÁM ĐỐC

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH NAM ĐỊNH

Vũ Trọng Quế

Phụ lục

Thông tin về các lỗ hổng bảo mật trong sản phẩm F5 BIG-IP

(Kèm theo Văn bản số .../STTTT-CĐS ngày .../11/2023 của Sở TT&TT)

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