**PHỤ LỤC**

**Thông tin về các lỗ hổng bảo mật**

*(Kèm theo Công văn số /STTTT-CNTT ngày /11/2023*

*của Sở Thông tin và Truyền thông tỉnh Đắk Lắk)*

 **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