Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT
(Kèm theo Công văn số /CATTT-NCSC ngày / /2022 của Cục An toàn thông tin)

1. Thông tin các lỗ hổng bảo mật

- Mô tả: Lỗ hổng ảnh hưởng đến FortiOS và FortiProxy, cho phép đối tượng tấn công chưa xác thực có quyền truy cập vào giao diện quản trị từ xa thông qua HTTP/HTTPS requests độc hại.

- Ảnh hưởng: FortiOS phiên bản 7.0.0 đến 7.0.6; 7.2.0 đến 7.2.1, FortiProxy phiên bản 7.0.0 đến 7.0.6, 7.2.0.

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 (FortiOS 7.0.7 và 7.2.2, FortiProxy 7.0.7 và 7.2.1). Trong trường hợp chưa thể nâng cấp, Quý đơn vị cần thực hiện biện pháp khắc phục tạm thời bằng cách thiết lập chính sách và hạn chế quyền truy cập các địa chỉ IP vào giao diện quản trị, triển khai xác thực đa yếu tố (MFA) để không bị lộ thông tin giao diện quản trị và tránh nguy cơ bị tấn công khai thác.

3. Tài liệu tham khảo

https://www.tenable.com/blog/cve-2022-40684-critical-authentication-bypass-in-fortios-and-fortiproxy

https://docs.fortinet.com/document/fortigate/7.2.2/fortios-release-notes/289806/resolved-issues

https://docs.fortinet.com/document/fortigate/7.2.0/best-practices/127480/user-authentication-for-management-network-access