UBND TỈNH TUYÊN QUANG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 1175 /STTTT-CNTT&BCVT
V/v lỗ hổng bảo mật ảnh hưởng nghiêm trọng trong FortiOS và FortiProxy

Tuyên Quang, ngày 14 tháng 10 năm 2022

Kính gửi:

- Văn phòng Đoàn Đại biểu Quốc hội và Hội đồng nhân dân;
- Văn phòng Ủy ban nhân dân tỉnh;
- Các sở, ban, ngành;
- Các tổ chức - Chính trị xã hội;
- Uỷ ban nhân dân các huyện, thành phố.

Căn cứ văn bản số 1547/CATTT-NCSC ngày 10/10/2022 của Cục An toàn thông tin về việc lỗ hổng bảo mật ảnh hưởng nghiêm trọng trong FortiOS và FortiProxy, Sở Thông tin và Truyền thông cung cấp thông tin và đưa ra các giải pháp phòng, tránh khai thác lỗ hổng bảo mật trong FortiOS và FortiProxy như sau:

I.Thông tin về lỗ hổng bảo mật trong FortiOS và FortiProxy

Ngày 07/10/2022, Fortinet đã công bố thông tin về lỗ hổng bảo mật CVE-2022-40684, ảnh hưởng nghiêm trọng trong các sản phẩm FortiOS và FortiProxy của mình. Lỗ hổng này cho phép đối tượng tấn công chưa xác thực chiếm quyền truy cập vào giao diện quản trị từ xa.

Thông tin chi tiết lỗ hổng bảo mật có tại Phụ lục gửi kèm theo.

Qua công tác giám sát an toàn không gian mạng quốc gia, 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 này đã được một số nhóm tấn công mạng sử dụng để tấn công vào hệ thống thông tin của nhiều cơ quan, tổ chức. Vì vậy, mức độ ảnh hưởng của lỗ hổng CVE-2022-40684 là 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.

2. Các giải pháp phòng tránh

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, Sở Thông tin và Truyền thông khuyến nghị Quý đơn vị thực hiện:

1. Kiểm tra, rà soát các sản phẩm FortiOS và FortiProxy 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 thiết lập chính sách để hạn chế quyền truy cập các địa chỉ IP vào giao diện quản trị (tham khảo thông tin tại Phụ lục gửi kèm theo).

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

3. 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 02432091616, thư điện tử: ais@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Ban Giám đốc sở (báo cáo);
- Các đơn vị thuộc sở;
- Lưu: VT, CNTT&BCVT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH TUYÊN QUANG

Nguyễn Văn Hiến

Phụ lục
THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT
(Kèm theo Công văn số 1175*/STTTT-CNTT&BCVT ngày* 14 */ 10 /2022*
của Sở Thông tin và Truyền thông)

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