TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM
LIÊN ĐOÀN LAO ĐỘNG TỈNH KHÁNH HÒA

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

Số: 383 /LĐ

Khánh Hòa, ngày 14 tháng 10 năm 2022

V/v lỗ hổng bảo mật có mức ảnh hưởng nghiêm trọng trong FortiOS và FortiProxy

Kính gửi:
- Các ban, đơn vị trực thuộc Liên đoàn Lao động tỉnh;
- Công đoàn cấp ngành;
- Liên đoàn Lao động cấp huyện;
- Các Công đoàn cơ sở trực thuộc.

Thực hiện Công văn số 2990/STTTT-CNTTBCVT, ngày 12/10/2022 của Sở Thông tin và Truyền thông và Công văn số 1547/CATTT-NCSC, ngày 10/10/2022 của Cục An toàn thông tin về việc lỗ hổng bảo mật có mức ảnh hưởng nghiêm trọng trong FortiOS và FortiProxy.

Theo nội dung Công văn số 1547/CATTT-NCSC, ngày 10/10/2022, 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 định chiếm quyền truy cập vào giao diện quản trị từ xa.

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, cần thực hiện rà soát và nâng cấp phiên bản hoặc áp dụng biện pháp khắc phục thay thế ngay lập tức.

Việc khai thác thành công lỗ hổng nêu trên có thể cho phép đối tượng thực thi mã từ xa, tấn công nâng cao đặc quyền trong hệ thống mục tiêu, từ đó có thể chiếm quyền điều khiển toàn bộ hệ thống.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các ban, đơn vị, Công đoàn cấp ngành, Liên đoàn Lao động cấp huyện, các Công đoàn cơ sở trực thuộc, Ban Thường vụ Liên đoàn Lao động tỉnh Khánh Hòa đề nghị các ban, đơn vị, Công đoàn cấp ngành, Liên đoàn Lao động cấp huyện, các Công đoàn cơ sở trực thuộc thực hiện một số nội dung sau:

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 theo hướng dẫn tại Phụ lục kèm theo Công văn số 1547/CATTT-NCSC (*gửi kèm Công văn này*).

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; 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. Khẩn trương thông báo nội dung văn bản này đến tất cả các Công đoàn cơ sở trực thuộc để tổ chức triển khai thực hiện.

4. Gửi kết quả thực hiện về Văn phòng Liên đoàn Lao động tỉnh qua hộp thư: ldldtinhkhanhhoa@gmail.com trước ngày 25/10/2022.

Quá trình thực hiện nếu có vướng mắc, đề nghị các ban, đơn vị, Công đoàn cấp ngành, Liên đoàn Lao động cấp huyện, các Công đoàn cơ sở trực thuộc liên hệ đầu mối thường trực Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa (điện thoại: 0258.3563533 - Thư điện tử: cntt.stttt@khanhhoa.gov.vn) để được hướng dẫn, hỗ trợ.

Ban Thường vụ Liên đoàn Lao động tỉnh Khánh Hòa đề nghị các ban, đơn vị, Công đoàn cấp ngành, Liên đoàn Lao động cấp huyện, các Công đoàn cơ sở trực thuộc quan tâm thực hiện./.

***Nơi nhận*:**
- Như kính gửi;
- Sở Thông tin và Truyền thông Khánh Hòa (b/c);
- Thường trực LĐLĐ tỉnh;
- Lưu Văn thư.

TL. BAN THƯỜNG VỤ
PHÓ CHÁNH VĂN PHÒNG

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM
BAN CHẤP HÀNH LIÊN ĐOÀN LAO ĐỘNG TỈNH KHÁNH HÒA

Huỳnh Thị Nam Khánh

Phụ lục

THÔNG TIN VỀ CÁC LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số 1547/CATTT-NCSC ngày 10 /10 /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