BỘ THÔNG TIN TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

Số: 1730 /CATTT-NCSC
V/v lỗ hổng bảo mật CVE-2021-41024 trong FortiOS và FortiProxy

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

Hà Nội, ngày 09 tháng 12 năm 2021

Kính gửi:

- Đơn vị chuyên trách về CNTT các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước; Các Ngân hàng TMCP; Các tổ chức tài chính;
- Hệ thống các đơn vị chuyên trách về an toàn thông tin.

Ngày 08/12/2021 vừa qua, Fortinet vừa công bố lỗ hổng bảo mật **CVE-2021-41024** trong FortiOS và FortiProxy, ảnh hưởng đến FortiGate phiên bản 7.0.1 và 7.0.0, FortiProxy phiên bản 7.0.0. Lỗ hổng này có điểm CVSS: 7.3 (cao), cho phép đối tượng có thể thực hiện tấn công mà không cần xác thực Directory traversal.

Theo đánh giá của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin, các sản phẩm của Fortinet được sử dụng rộng rãi ở nhiều cơ quan, tổ chức, doanh nghiệp tại Việt Nam để thuận tiện trong việc quản lý và bảo đảm an toàn thông tin hệ thống. Vì vậy, lỗ hổng này có thể gây ảnh hưởng lớn đến hệ thống thông tin của nhiều cơ quan, tổ chức, doanh nghiệp.

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, Cục An toàn thông tin khuyến nghị Quý đơn vị thực hiện:

1. Kiểm tra, rà soát và xác minh hệ thống thông tin có sử dụng FortiOS và FortiProxy hay không. Nếu có, Quý đơn vị cần cập nhật lên phiên bản mới nhất (FortiGate phiên bản 7.0.2 trở lên, FortiProxy phiên bản 7.0.1 trở lên) để khắc phục lỗ hổng bảo mật nói trên cũng như các lỗ hổng bảo mật mới phát hiện khác.

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 hỗ trợ, Quý đơn vị liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại: 02432091616, thư điện tử: ncsc@ais.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Huy Dũng (để b/c);
- Cục A05, Bộ Công an;
- Bộ Tư lệnh 86, Bộ Quốc phòng;
- Ban Cơ yếu Chính phủ;
- Cục trưởng;
- Lưu: VT, NCSC.

CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Thành Phúc

Phụ lục

THÔNG TIN LỖ HỔNG BẢO MẬT

(Kèm theo Công văn số /CATTT-NCSC ngày / /2021 của Cục An toàn thông tin)

1. Thông tin lỗ hổng bảo mật

- Mô tả: Lỗ hổng này ảnh hưởng đến FortiOS và FortiProxy, cho phép đối tượng tấn công không cần xác thực, có thể thực hiện tấn công directory traversal.

- Điểm CVSS: 7.3 (cao)

- Ảnh hưởng: FortiGate phiên bản 7.0.1 và 7.0.0, FortiProxy phiên bản 7.0.0.

2. Hướng dẫn khắc phục

Fortinet đã phát hành bản vá cho lỗ hổng bảo mật này tại FortiGate phiên bản 7.0.2 trở lên, FortiProxy phiên bản 7.0.1 trở lên. Vì vậy để khắc phục và tránh nguy cơ tấn công, Quý đơn vị cần cập nhật bản vá trong thời gian sớm.

3. Nguồn tham khảo

https://www.fortiguard.com/psirt/FG-IR-21-181