UBND THÀNH PHỐ HẢI PHÒNG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 119 /STTTT-CNTT
V/v cảnh báo lỗ hổng bảo mật trên sản phẩm FortiWeb.

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

Hải Phòng, ngày 20 tháng 01 năm 2021

Kính gửi:
- Các Sở, ban, ngành thành phố;
- Các cơ quan Trung ương tổ chức theo ngành dọc;
- Ủy ban nhân dân các quận, huyện;
- Các tổ chức, doanh nghiệp trên địa bàn.

Ngày 11/01/2021, Cục An toàn thông tin có Công văn số 18/CATTT-NCSC về việc cảnh báo 04 lỗ hổng bảo mật (CVE-2020-29015, CVE-2020-29016, CVE-2020-29018, CVE-2020-29019) trên sản phẩm FortiWeb, hướng dẫn cách khắc phục lỗ hổng trên *(gửi kèm văn bản)*.

Sở Thông tin và Truyền thông trân trọng đề nghị các cơ quan, đơn vị kiểm tra, rà soát hệ thống công nghệ thông tin và thực hiện các biện pháp phát hiện, ngăn chặn nguy cơ gây mất an toàn thông tin do lỗ hổng trên sản phẩm FortiWeb gây ra tại cơ quan và các đơn vị trực thuộc theo hướng dẫn của Cục An toàn thông tin tại Công văn số 18/CATTT-NCSC.

Sở Thông tin và Truyền thông cử ông Nguyễn Đông Huy (Trưởng Phòng Hạ tầng kỹ thuật và An toàn thông tin - Trung tâm Thông tin và Truyền thông, số điện thoại 098.4462472) là đầu mối phối hợp, trao đổi thông tin.

Trân trọng./.

Nơi nhận:
- Như trên;
- UBNDTP (để b/c);
- Ban 114 (để b/c);
- GĐ, các PGĐ Sở;
- Trung tâm TT&TT;
- Cổng TTĐT Sở, Cổng Tin tức TP;
- Lưu: VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
THÀNH PHỐ HẢI PHÒNG

Lê Văn Kiên

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

Số: 18 /CATTT-NCSC
V/v cảnh báo lỗ hổng bảo mật trên sản phẩm FortiWeb

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

Hà Nội, ngày 11 tháng 01 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.

Qua công tác theo dõi, giám sát trên không gian mạng, cùng hoạt động hợp tác, chia sẻ thông tin với các tổ chức lớn về an toàn thông tin trong và ngoài nước, Cục An toàn thông tin ghi nhận **04 lỗ hổng bảo mật (CVE-2020-29015, CVE-2020-29016, CVE-2020-29018, CVE-2020-29019)** trên sản phẩm FortiWeb (thông tin chi tiết về lỗ hổng có tại phụ lục kèm theo).

FortiWeb là giải pháp bảo mật chuyên dụng toàn diện cho hệ thống ứng dụng web, thường sử dụng trong các hệ thống thông tin của các cơ quan tổ chức để giám sát mạng, hệ thống và cơ sở hạ tầng công nghệ thông tin. Theo đánh giá sơ bộ, lỗ hổng này có thể ảnh hưởng đến nhiều cơ quan, tổ chức ở Việt Nam, đặc biệt là cơ quan chính phủ, ngân hàng, tổ chức tài chính, tập đoàn, doanh nghiệp và các công ty lớn, do các đơn vị này đều triển khai mô hình mạng có sử dụng FortiWeb để thuận tiện cho việc quản lý và bảo mật ATTT cho hệ thống.

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 đề nghị quý đơn vị thực hiện:

1. Rà soát xác minh hệ thống web có sử dụng FortiWeb để phát hiện và xử lý kịp thời các lỗ hổng bảo mật, đặc biệt là các lỗ hổng có tại phụ lục kèm theo.

2. Cập nhật bản vá hoặc khắc phục lỗ hổng bảo mật đồng thời thường xuyên thực hiện kiểm tra đánh giá, bảo đảm an toàn thông tin.

3. Tăng cường theo dõi giám sát hệ thống đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn để phát hiện kịp thời các nguy cơ tấn công mạng.

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;
- Thứ trưởng Nguyễn Huy Dũng (để b/c);
- Cục trưởng (để b/c);
- PCT Nguyễn Khắc Lịch;
- Lưu: VT, NCSC.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

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

Nguyễn Khắc Lịch

Phụ lục

Thông tin các lỗ hổng

(Kèm theo Công văn số 18 /CATTT-NCSC ngày 11 /01 /2020)

1. CVE-2020-29015

- Mức độ: trung bình (CVSS: 6.4)

- Lỗ hổng tồn tại trong giao diện người dùng của FortiWeb, cho phép đối tượng tấn công chèn và thực thi mã từ xa, tấn công SQL injection.

Khai thác lỗ hổng bảo mật này cho phép đối tượng tấn công đọc, xóa, sửa đổi dữ liệu, chiếm quyền kiểm soát hệ thống ứng dụng mục tiêu.

- Ảnh hưởng: FortiWeb phiên bản <6.3.7 và <6.2.3

- Giải pháp: nâng cấp lên phiên bản >6.3.8 và >6.2.4

Truy cập tại: https://support.fortinet.com/

2. CVE-2020-29019

- Mức độ: trung bình (CVSS:6.4)

- Lỗ hổng trong FortiWeb cho phép đối tượng tấn công chèn và thực thi mã từ xa, làm tràn bộ đệm.

- Ảnh hưởng: phiên bản <6.4.7 và <6.2.3

- Giải pháp: nâng cấp lên phiên bản > 6.3.8 và >6.2.4

Truy cập tại: https://support.fortinet.com/

3. CVE-2020-29018

- Mức độ: trung bình (CVSS: 5.3)

- Lỗ hổng cho phép đối tượng tấn công chèn và thực thi mã tùy ý, đánh cắp thông tin dữ liệu nhạy cảm.

- Ảnh hưởng: phiên bản < 6.3.5

- Giải pháp: nâng cấp lên phiên bản > 6.3.6

Truy cập tại: https://support.fortinet.com/

4. CVE-2020-29016

- Mức độ: trung bình (CVSS: 6.4)

- Lỗ hổng cho phép đối tượng tấn công chèn và thực thi mà tùy ý, làm tràn bộ đệm.

Truy cập tại: https://support.fortinet.com/