BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

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

Số: 07 /TTCNTT-KTHT
V/v cảnh báo lỗ hổng bảo mật trên sản phẩm FortiWeb

Hà Nội, ngày 15 tháng 01 năm 2021

Kính gửi: Các đơn vị có hệ thống công nghệ thông tin trực thuộc Bộ

Theo thông báo của Cục An toàn thông tin – Bộ Thông tin và Truyền thông, 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 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, Trung tâm Công nghệ 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 thông tin 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 Trung tâm Công nghệ thông tin: Phòng Kỹ thuật hạ tầng, điện thoại 024.39439060, thư điện tử: phongktht@most.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Bùi Thế Duy (để biết);
- Lưu: VT, KTHT.

GIÁM ĐỐC

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Hà Quốc Trung

Phụ lục
Thông tin các lỗ hổng
(Kèm theo Công văn số /TTCNTT-KTHT ngày / /2021)

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.

- Ảnh hưởng: phiên bản < 6.3.5 và <6.2.3

- Giải pháp: nâng cấp lên phiên bản > 6.3.6 và >6.2.4

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