UBND TỈNH TUYÊN QUANG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 33 /STTTT-CNTT
Về việc cảnh báo lỗ hổng bảo mật trên sản phẩm FortiWeb

Tuyên Quang, ngày 19 tháng 01 năm 2021

Kính gửi:
- Văn phòng Hội đồng nhân dân tỉnh;
- Văn phòng Ủy ban nhân dân tỉnh;
- Các sở, ban, ngành;
- Uỷ ban nhân dân các huyện, thành phố;
- Trung tâm Công nghệ thông tin và Truyền thông, Sở Thông tin và Truyền thông.

Thực hiện Văn bản số 18/CATTT-NCSC ngày 11/01/2021 của Cục An toàn thông tin về việc cảnh báo lỗ hổng bảo mật trên sản phẩm FortiWeb; Sở Thông tin và Truyền thông cung cấp thông tin và đưa ra các giải pháp phòng, tránh việc khai thác lỗ hổng bảo mật trên sản phẩm FortiWeb, cụ thể như sau:

I. Thông tin về lỗ hổng bảo mật trên sản phẩm FortiWeb

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.

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).

II. 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 đề nghị các sở, ban, ngành, Ủy ban nhân dân các huyện, thành phố triển khai thực hiện các giải pháp sau:

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;
- Ban Giám đốc sở (báo cáo);
- Lưu: VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

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

Sở Thông tin và Truyền thông
19-01-2021 15:39:39 +07:00

Nguyễn Văn Hiến

PHỤ LỤC
THÔNG TIN VỀ LỖ HỔNG BẢO MẬT TRÊN SẢN PHẨM FORTIWEB
(Kèm theo Công văn số 33 /STTTT-CNTT ngày 19 /01/2021 của Sở Thông tin và Truyền thông)

STT	CVE	Mô tả
1	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	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	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	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/