BỘ Y TẾ
CỤC CÔNG NGHỆ THÔNG TIN

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

Số: 222/CNTT-THDL
V/v cảnh báo lỗ hổng an toàn thông tin hệ quản trị nội dung Drupal

Hà Nội, ngày 24 tháng 4 năm 2018

Kính gửi:

- Tổng Cục Dân số-KHHGĐ, Văn phòng Bộ, Thanh tra Bộ và các Vụ, Cục thuộc Bộ Y tế;
- Các đơn vị trực thuộc Bộ Y tế;
- Sở Y tế các tỉnh, thành phố trực thuộc Trung ương.

Căn cứ Công văn số 109/VNCERT-KTHT&GS của Trung tâm Ứng cứu khẩn cấp Máy tính Việt Nam ngày 24/4/2018 về việc cảnh báo lỗ hổng an toàn thông tin hệ quản trị nội dung Drupal, Cục Công nghệ thông tin đề nghị các đơn vị kiểm tra để phát hiện và xử lý triệt để 02 lỗ hổng an toàn thông tin đối với các website có sử dụng Hệ quản trị nội dung Drupal (Drupal CMS) theo mô tả và hướng dẫn dưới đây.

1. Lỗ hổng Drupal cho phép thực thi các lệnh điều khiển từ xa trái phép (Remote Code Execution)

***1.1 Mã lỗi quốc tế*:** CVE-2018-7600 hoặc SA-CORE-2018-002

1.2 Mức độ nghiêm trọng: Nghiêm trọng

Mức độ nguy hiểm là nghiêm trọng do:

+ Khi khai thác thành công, tin tặc sẽ dễ dàng cài đặt các phần mềm mã độc, phần mềm khai thác, phần mềm điều khiển trái phép toàn quyền điều khiển hệ thống.

+ Kỹ thuật khai thác rất dễ thực hiện, không yêu cầu bất cứ điều kiện gì kèm thêm.

+ Không yêu cầu quyền truy cập hệ thống.

+ Có thể sửa và xóa dữ liệu.

+ Máy tính bị khai thác có thể trở thành bàn đạp khai thác các máy tính khác trong cùng vùng mạng.

1.3 Thời điểm công bố lỗ hổng: 28/3/2018

1.4 Thời điểm công bố mã khai thác: 13/4/2018 một số webiste đã công bố mã khai thác thí điểm lỗ hổng.

1.5 Mô tả ảnh hưởng: cho phép tin tặc tấn công từ xa, tải tệp tin trái phép, thay đổi giao diện v.v.., lỗ hổng tồn tại trên nhiều phiên bản khác nhau của Drupal, xem chi tiết trong phần giải pháp xử lý sự cố.

Hiện nay ảnh hưởng trên diện rộng đã có một số hacker khai thác lỗ hổng Drupal để phục vụ đào tiền ảo.

1.6 Giải pháp xử lý

1. Cập nhật Drupal

Drupal đã cung cấp khá đầy đủ các bản vá và xử lý lỗi cho lỗ hổng CVE-2018-7600 hoặc SA-CORE-2018-002, quản trị hệ thống xem xét xử lý theo hướng dẫn được tổng hợp từ Drupal như sau:

- Nếu sử dụng Drupal 7.x cần nâng cấp phiên bản 7.5.8. Trong trường hợp không nâng cấp ngay lập tức thì cài đặt bản vá link dưới đây: https://cgit.drupalcode.org/drupal/rawdiff/?h=7.x&id=2266d2a83db50e2f97682d9a0fb8a18e2722cba5

- Nếu sử dụng phiên bản Drupal 8.5.x thì cập nhật lên phiên bản 8.5.1. Trong trường hợp không nâng cấp ngay lập tức thì cài đặt bản vá link dưới đây https://cgit.drupalcode.org/drupal/rawdiff/?h=8.5.x&id=5ac8738fa69df34a0635f0907d661b509ff9a28f

- Nếu đang sử dụng các phiên bản Drupal 8.3 hoặc 8.4 thì nhanh chóng nâng cấp lên phiên bản 8.5.1. Trong trường hợp không thể thực hiện thì có thể sử dụng hai biện pháp tạm thời sau (tuy nhiên các biện pháp này vẫn còn tiềm ẩn nhiều rủi ro khác):

+ Nếu đang sử dụng Drupal 8.3.x thì nâng cấp lên phiên bản 8.3.9 và cài đặt bản vá tại đường dẫn sau đây
https://cgit.drupalcode.org/drupal/rawdiff/?h=8.5.x&id=5ac8738fa69df34a0635f0907d661b509ff9a28f

+ Nếu đang sử dụng Drupal 8.4.x thì nâng cấp lên phiên bản 8.4.6 và cài đặt bản vá tại đường dẫn sau đây
https://cgit.drupalcode.org/drupal/rawdiff/?h=8.5.x&id=5ac8738fa69df34a0635f0907d661b509ff9a28f

2. Các giải pháp hỗ trợ khác

Thiết lập thiết bị IPS, tường lửa bảo vệ lớp 7 hoặc tường lửa bảo vệ ứng dụng web (Web Application firewall) và cập nhật đầy đủ thông tin để có thể ngăn chặn được các tấn công lỗ hổng.

Với các thiết bị chưa được nhà sản xuất cập nhật khả năng ngăn chặn tấn công CVE-2018-7600 (hoặc SA-CORE-2018-002), thì tham khảo đoạn mã phát hiện tấn công sau được viết cho phần mềm phát hiện xâm nhập nguồn mở Snort:

alert http $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"Drupalgeddon2 (CVE-2018-7600)"; flow: to_server,established; content:"POST"; http_method; content:"markup"; fast_pattern; content:

"/user/register"; http_uri; pcre:"/(access_callback|pre_render|lazy_builder|post_render)/i"; classtype:web-application-attack; sid:9000110; rev:1

2. Lỗ hổng tấn công kịch bản liên trang (Cross Site Scriptting)

2.1 Mã hỗi quốc tế: SA-CORE-2018-003

2.2 Mức độ nghiêm trọng: Cao

2.3 Thời điểm công bố: 18/4/2018

2.4 Mô tả ảnh hưởng

Ứng dụng CKEditor là một ứng dụng xây dựng trên nền tảng Java Script được tích hợp với phần mềm Drupal, ứng dụng này đã xuất hiện lỗ hổng cho phép khả năng khai thác lỗi Cross Site Scripting (XSS). Lỗ hổng này cho phép tin tặc thực thi các XSS thông qua CKEditor khi có sử dụng Plugin Image2 (Plugin này cũng được sử dụng trong phiên bản Drupal 8).

2.5 Giải pháp xử lý

1. Sử dụng Drupal 8, cần nâng cấp lên bản 8.5.2 hoặc 8.4.7

2. Sử dụng Drupal 7.x, chỉ bị ảnh hưởng bởi lỗ hổng trên nếu sử dụng CKEditor module 7.x-1.18 hoặc CKEditor từ CDN.

3. Nếu cài đặt CKEditor với Drupal 7 bằng các phương thức riêng như (sử dụng WYSIWYG module, CKEditor locally) và sử dụng các phiên bản CKEditor từ 4.5.11 tới 4.9.1, thì cần cập nhật thư viện third-party JavaScript library tại địa chỉ https://ckeditor.com/ckeditor-4/download/

Việc cập nhật phần mềm Drupal cho các website/cổng thông tin điện tử có thể dẫn đến một số trục trặc trong khi đây là phần mềm mã nguồn mở nên việc hỗ trợ từ cộng đồng và nhà sản xuất còn hạn chế. Do đó cần thử nghiệm và nghiên cứu kỹ trước khi thực hiện các biện pháp cập nhật cho các hệ thống lớn, yêu cầu tính sẵn sàng cao để hạn chế rủi ro.

Mọi thông tin chi tiết và đề nghị hỗ trợ kỹ thuật vui lòng liên hệ đầu mối của Trung tâm Tích hợp Dữ liệu: Ông Phạm Hữu Thảo – Phụ trách Phòng Hạ tầng và An toàn thông tin; email: thaoph.cntt@moh.gov.vn; điện thoại: 0944701619.

Trân trọng./.

Nơi nhận:
- Như trên;
- PCT. Lương Chí Thành (để biết);
- Lưu: VT, THDL.

CỤC TRƯỞNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
CỤC CÔNG NGHỆ THÔNG TIN
BỘ Y TẾ

Trần Quý Tường