BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

Số: 109/VNCERT-KTHT&GS
V/v cảnh báo lỗ hổng an toàn thông tin hệ quản trị nội dung Drupal

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

Hà Nội, ngày 23 tháng 4 năm 2018

KHẨN

Kính gửi:

- Các đơn vị chuyên trách về CNTT, ATTT: Văn phòng Trung ương Đảng, Văn phòng Chủ tịch nước, Văn phòng Quốc hội, Văn phòng Chính phủ;
- Các đơn vị chuyên trách về CNTT, ATTT các Bộ, ngành;
- Các Sở Thông tin và Truyền thông;
- Các Thành viên Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia;
- Các Tổng công ty, Tập đoàn kinh tế; các tổ chức Tài chính, Ngân hàng và Chứng khoán; các Doanh nghiệp hạ tầng Internet, Viễn thông, Điện lực, Hàng không, Giao thông vận tải, Dầu khí;
- Các đơn vị thuộc Bộ Thông tin và Truyền thông.

Hệ quản trị nội dung Drupal (Drupal CMS) mã nguồn mở hiện là một trong các hệ quản trị nội dung được sử dụng khá phổ biến để xây dựng các trang/cổng thông tin điện tử, ứng dụng web (gọi chung là Website)cho các cơ quan đơn vị với các ưu điểm là đơn giản, linh hoạt hỗ trợ nhiều loại CSDL như MySQL, PostgreSQL, SQLite, MS SQL Server, Oracle và có thể mở rộng để hỗ trợ các CSDL NoSQL.

Trong hai năm 2017 và 2018, Drupal đã công bố 7 lỗ hổng bảo mật, nhưng chỉ riêng từ cuối tháng 3 đến nay đã bộc lộ 2 lỗ hổng bảo mật có mức độ nguy hiểm cao đến nghiêm trọng cần được theo dõi xử lý khẩn cấp. Số lượng website Drupal tại Việt nam là khá nhiều nhưng Drupal thường được sử dụng đối với các website có quy mô vừa và nhỏ. Drupal ít được sử dụng cho các hệ thống nghiệp vụ quan trọng của các tổ chức Ngân hàng, tài chính. Qua công tác hỗ trợ một số đơn vị khắc phục sự cố do Drupal vừa qua, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam nhận thấy thực tế website do đối tác bên ngoài xây dựng không bàn giao đầy đủ nên đơn vị vận hành website, thậm chí cả cán bộ kỹ thuật chủ chốt không biết rõ cổng/trang thông tin điện tử được phát triển trên nền tảng Drupal nên dẫn đến tình trạng chủ quan, bỏ qua lỗ hổng an toàn thông tin đã được cảnh báo, có thể bị tấn công gây mất an toàn thông tin. Do đó kính đề nghị các cơ quan, tổ chức quan tâm kiểm tra để phát hiện triệt để các website có sử dụng Drupal.

Trong trường hợp có website sử dụng Drupal thì cần chú ý hai lỗ hổng an toàn thông tin sau 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 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:

1. Khi 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

2. 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

3. 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):

a. 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

b. 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

1.7 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 đó 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 VNCERT: Ông Nguyễn Thanh Minh – Phụ trách Phòng Kỹ thuật hệ thống và Giám sát; email: ntminh@vncert.vn; điện thoại: 0904240888.

Trân trọng./.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

Ngô Quang Huy

Nơi nhận:
- Như trên;
- Thứ trưởng Nguyễn Thành Hưng (để b/c);
- Giám đốc (để b/c);
- PGĐ Nguyễn Khắc Lịch (để p/h);
- Các phòng, chi nhánh: ĐPƯC, NCPT, TVĐT, CNHCM, CNĐN;
- Lưu VT, KTHT&GS.