

**TỔNG CỤC THỐNG KÊ
CỤC THU THẬP DỮ LIỆU
VÀ ỨNG DỤNG CÔNG NGHỆ THÔNG TIN**

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

Số: 230 /TTDL-CNTT

Hà Nội, ngày 09 tháng 10 năm 2024

V/v rà soát, khắc phục lỗ hổng
trên các trang web

Kính gửi:

- Cục Thống kê tỉnh, thành phố trực thuộc trung ương;
- Thành viên Tổ ứng cứu sự cố;
- Trung tâm Tin học thống kê khu vực I, II, III.

Ngày 03/10/2024, Cục Thu thập dữ liệu và Ứng dụng công nghệ thông tin thống kê (Cục TTDL) ghi nhận trang thông tin điện tử của Cục Thống kê tỉnh Bình Thuận đã bị tin tặc khai thác qua lỗ hổng bảo mật của trình soạn thảo văn bản FCKeditor để chèn đường dẫn có nội dung phản cảm. Để đảm bảo an toàn cho hệ thống thông tin, Cục TTDL đề nghị các đơn vị thực hiện:

1. Kiểm tra, rà soát hệ thống thông tin thuộc phạm vi quản lý, đặc biệt là các lỗ hổng bảo mật cơ bản như: SQL Injection, FckEditor, WebDAV, mật khẩu yếu...;
2. Thường xuyên theo dõi, giám sát, cập nhật các bản vá bảo mật mới nhất cho các nền tảng, các plugin, module trong ứng dụng để phòng ngừa, ngăn chặn có hiệu quả các thủ đoạn, hoạt động tấn công xâm nhập của tin tặc các trang thông tin điện tử;
3. Chuẩn bị các phương án xử lý kịp thời khi phát hiện có dấu hiệu hệ thống thông tin bị tấn công;
4. Cục Thống kê tỉnh Bình Thuận khẩn trương tổ chức khắc phục sự cố bảo mật theo hướng dẫn tại Phụ lục kèm theo.

Trong quá trình triển khai, có khó khăn, vướng mắc đề nghị liên hệ với Trung tâm Tin học thống kê khu vực phụ trách để được trợ giúp. Kết quả thực hiện đề nghị các đơn vị gửi về Cục TTDL **chậm nhất ngày 17/10/2024** để tổng hợp chung.

Trân trọng cảm ơn sự phối hợp của Quý Đơn vị./. 

Nơi nhận:

- Như trên;
- Lãnh đạo Tổng cục (để b/c);
- Cục trưởng (để b/c);
- Lưu VT, CNTT.

**KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG**




Cao Quang Thành

Phụ lục
HƯỚNG DẪN KHẮC PHỤC LỖ HỔNG TRONG FCKEDITOR
(Kèm theo Công văn số: /TTDL-CNTT ngày tháng 10 năm 2024 của Cục
Thu thập dữ liệu và Ứng dụng công nghệ thông tin thống kê)

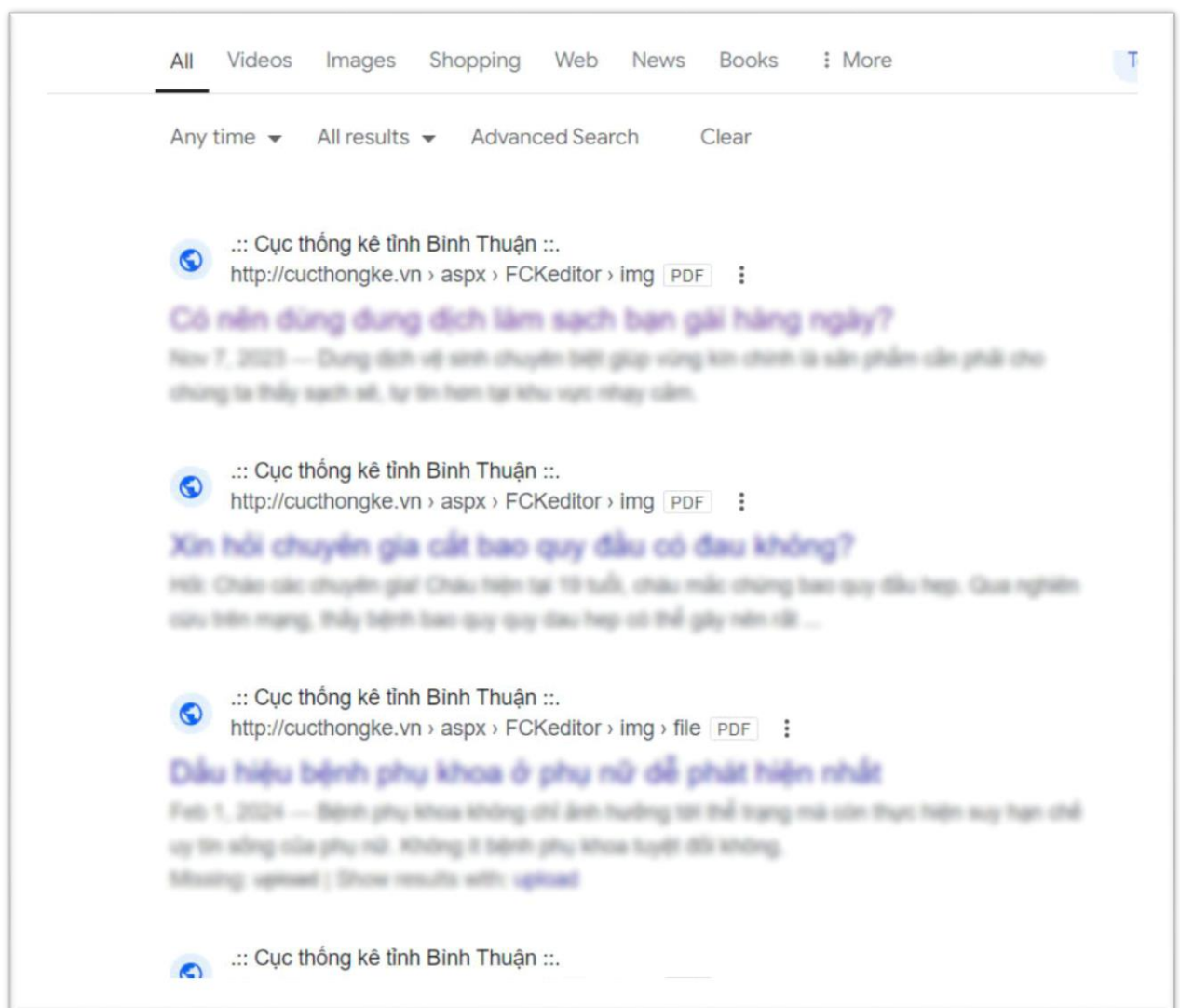
1. Hướng dẫn rà quét

Mở trình duyệt và vào trang tìm kiếm “google.com”

Nhập nội dung tìm kiếm: **inurl:FCKeditor editor filemanager upload site:cucthongke.vn**

Trong đó **cucthongke.vn** là tên miền, đơn vị rà quét theo tên miền của trang web cần rà quét.

2. Lỗ hổng tại website Cục Thống kê tỉnh Bình Thuận



3. Hướng dẫn khắc phục

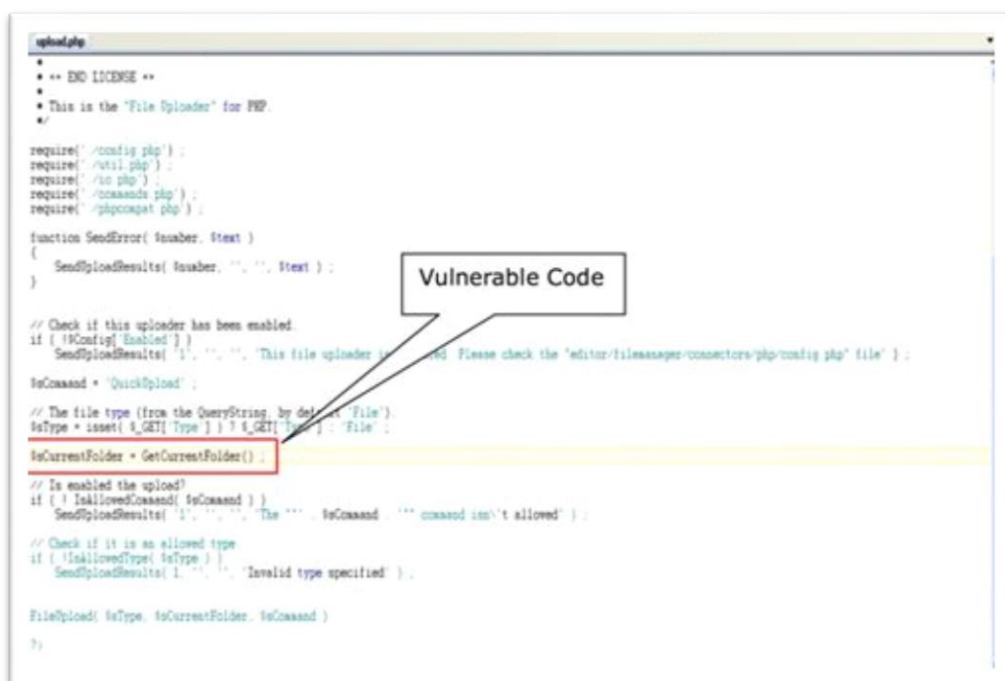
FCKeditor (còn gọi là CKEditor) là một trình soạn thảo HTML mã nguồn mở theo kiểu WYSIWYG của CKSource. Chương trình này có thể tích hợp vào

các web site mà không cần cài đặt. CKEditor tương thích với hầu hết các trình duyệt Internet và được sử dụng rất rộng rãi.

Lỗi chủ yếu do các website đang dùng bản cũ và không xóa các form upload test mặc định có trong FCKEditor. Khi triển khai FCKEditor chưa cấu hình phân quyền thư mục, phân quyền thực thi trong các thư mục upload của Web Server. Kẻ tấn công có thể lợi dụng để upload các file với nội dung xấu lên website hoặc upload các webshell lên Website nhằm chiếm quyền điều khiển website.

Để khắc phụ lỗi này, quản trị website nên thực hiện các công việc sau:

- Xóa các thư mục upload test trên website.
- Cấu hình phân quyền thư mục, phân quyền thực thi theo kiểu file trong thư mục upload.
- Có thể cập nhật phiên bản mới của FCKEditor
- Bạn cũng có thể khắc phục thủ công bằng cách thay đổi trực tiếp mã nguồn trong tệp tin upload.php. Thay đổi 'sCurrentFolder = GetCurrentFolder()' thành 'sCurrentFolder = "/"'.



```

upload.php
*
* ** END LICENSE **
*
* This is the "File Uploader" for PHP.
*
require( './config.php' );
require( './util.php' );
require( './io.php' );
require( './commands.php' );
require( './phpcompat.php' );

function SendError( $number, $text )
{
    SendUploadResults( $number, "", "", $text );
}

// Check if this uploader has been enabled.
if ( ! $Config[ 'Enabled' ] )
{
    SendUploadResults( '1', "", "", "This file uploader is disabled. Please check the 'editor/filemanager/connectors/php/config.php' file" );
}

$sCommand = 'QuickUpload';

// The file type (from the QueryString, by default 'File').
$type = isset( $_GET[ 'type' ] ) ? $_GET[ 'type' ] : 'File';

$sCurrentFolder = GetCurrentFolder();

// Is enabled the upload?
if ( ! IsAllowedCommand( $sCommand ) )
{
    SendUploadResults( '1', "", "", "The '" . $sCommand . "' command isn't allowed" );
}

// Check if it is an allowed type
if ( ! IsAllowedType( $type ) )
{
    SendUploadResults( '1', "", "", "Invalid type specified" );
}

FileUpload( $type, $sCurrentFolder, $sCommand );
?
  
```

Mã nguồn có lỗ hổng



The image shows a screenshot of a web browser displaying a PHP file named `upload.php`. The code is a file upload script. A callout box with the text "Safe Code" points to the line `$sCurrentFolder = "/";`, which is highlighted in yellow. The code includes comments, requires other PHP files, defines a `SendError` function, checks if the uploader is enabled, sets the command to "QuickUpload", and checks if the file type is allowed. The `$sCurrentFolder` variable is set to the root directory.

```

upload.php
* -- END LICENSE --
* This is the 'File Uploader' for FWP.
*/

require( './config.php' );
require( './util.php' );
require( './so.php' );
require( './commands.php' );
require( './phpconnect.php' );

function SendError( $number, $text )
{
    SendUploadResults( $number, '', '', $text );
}

// Check if this uploader has been enabled.
if ( !$Config[ 'Enabled' ] )
    SendUploadResults( '1', '', '', 'This file uploader is disabled. Please check the "editor/filemanager/connectors/php/config.php" file' );

$sCommand = 'QuickUpload';

// The file type (from the QueryString by default 'File').
$type = isset( $_GET[ 'type' ] ) ? $_GET[ 'type' ] : 'File';

$sCurrentFolder = "/";

// Is enabled the upload?
if ( ! $isAllowedCommand( $sCommand ) )
    SendUploadResults( '1', '', '', 'The "' . $sCommand . '" command isn\'t allowed' );

// Check if it is an allowed type.
if ( ! $isAllowedType( $type ) )
    SendUploadResults( '1', '', '', 'Invalid type specified' );

FileUpload( $type, $sCurrentFolder, $sCommand );
?>

```

Mã nguồn An toàn