FCKeditor ADS File Upload Vulnerability - Windows Only

2007-06-18 15:38:59 by Raven

SECUNIA ADVISORY ID: SA25719

VERIFY ADVISORY: http://secunia.com/advisories/25719/

CRITICAL: Moderately critical

IMPACT: Security Bypass

WHERE: >From remote

SOFTWARE: FCKeditor 2.x - http://secunia.com/product/7973/

DESCRIPTION: A vulnerability has been discovered in FCKeditor, which can be exploited by malicious people to bypass certain security restrictions.

The vulnerability is caused due to an error in the file upload functionality. This can be exploited to bypass the file extension filter and upload files with arbitrary extensions by using the NTFS Alternate Data Stream (ADS) as the filename, e.g. "file.php::$DATA". Successful exploitation requires that an NTFS file system is used and that file uploads have been enabled in the "config.php" configuration file (not enabled by default). The vulnerability is confirmed in version 2.4.3 using the PHP file uploader.

SOLUTION: Disable file uploads in config.php. Grant only trusted user access to the application.

PROVIDED AND/OR DISCOVERED BY: Michael Schramm

ORIGINAL ADVISORY: http://ha.ckers.org/blog/20070606/additional-image-bypass-on-windows/