tenable | Plugins

Nessus

Advanced Custom Fields Plugin for WordPress 'acf_abspath' Parameter Remote File Inclusion

HIGH Nessus Plugin ID 63326

Information | Dependencies | Dependents | Changelog

Synopsis

The remote web server contains a PHP application that is afffected by a remote file inclusion attack.

Description

The version of the Advanced Custom Fields plugin for WordPress installed on the remote host fails to properly sanitize user-supplied input to the 'acf_abspath' parameter of its 'core/actions/export.php' script. A remote, unauthenticated attacker can exploit this issue to view arbitrary files or execute arbitrary PHP code, possibly taken from third-party hosts, on the remote host.

Solution

Upgrade to Advanced Custom Fields version 3.5.2 or later.

See Also

http://www.nessus.org/u?91911f17

http://www.advancedcustomfields.com/to-do/#3.5.2

Plugin Details

Severity: High

ID: 63326

File Name: wordpress_advanced_custom_fields_rfi.nasl

Version: 1.12

Type: Remote

Family: CGI abuses

Published: 12/21/2012

Updated: 5/14/2025

Supported Sensors: Nessus

Enable CGI Scanning: true

Vulnerability Information

CPE: cpe:/a:wordpress:wordpress

Required KB Items: installed_sw/WordPress, www/PHP

Exploit Available: true

Exploit Ease: Exploits are available

Exploited by Nessus: true

Patch Publication Date: 11/16/2012

Vulnerability Publication Date: 11/14/2012

Exploitable With

Metasploit (WordPress Plugin Advanced Custom Fields Remote File Inclusion)

Elliot (WordPress Advanced Custom Fields 3.5.1 RFI)

Reference Information

BID: 56528

Community & Support

Documentation

Education

Privacy Policy

Legal

508 Compliance