IPS Community Suite 4.5.4.2 PHP Code Injection

Authored by EgiX | Site karmainsecurity.com

Posted May 31, 2021

IPS Community Suite versions 4.5.4.2 and below suffer from a PHP code injection vulnerability. The vulnerability exists because the IPS\cms\modules\front\pages_builder::previewBlock() method allows to pass arbitrary content to the IPS_Theme::runProcessFunction() method, which will be used in a call to the eval() PHP function. This can be exploited to inject and execute arbitrary PHP code. Successful exploitation of this vulnerability requires an account with permission to manage the sidebar (such as a Moderator or Administrator) and the "cms" application to be enabled.

tags | exploit, arbitrary, php
advisories | CVE-2021-32924
SHA-256 | 392b40ad40c330e4deb04c99f4ff988666d96d0c4e3c606a17ec99241047911a Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
------------------------------------------------------------------------------
IPS Community Suite <= 4.5.4.2 (previewBlock) PHP Code Injection
Vulnerability
------------------------------------------------------------------------------


[-] Software Link:

https://invisioncommunity.com


[-] Affected Versions:

Version 4.5.4.2 and prior versions.


[-] Vulnerability Description:

The vulnerability exists because the
IPS\cms\modules\front\pages\_builder::previewBlock() method allows to
pass arbitrary content to the IPS\_Theme::runProcessFunction() method,
which will be used in a call to the eval() PHP function. This can be
exploited to inject and execute arbitrary PHP code. Successful
exploitation of this vulnerability requires an account with permission
to manage the sidebar (such as a Moderator or Administrator) and the
"cms" application to be enabled.


[-] Proof of Concept:

http://[host]/[ips]/index.php?
app=cms&module=pages&controller=builder&do=previewBlock&block_plugin=stats&block_template_use_how=copy&block_pl


[-] Solution:

Apply the vendor patch or upgrade to version 4.6.0 or later.


[-] Disclosure Timeline:

[02/02/2021] - Vendor notified through HackerOne
[02/04/2021] - Asked for an update
[06/04/2021] - Vendor replies they already released a targeted patch
[13/05/2021] - CVE number assigned
[28/05/2021] - Public disclosure


[-] CVE Reference:

The Common Vulnerabilities and Exposures project (cve.mitre.org)
has assigned the name CVE-2021-32924 to this vulnerability.


[-] Credits:

Vulnerability discovered by Egidio Romano.


[-] Other References:

https://hackerone.com/reports/1092574


[-] Original Advisory:

http://karmainsecurity.com/KIS-2021-04
```

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