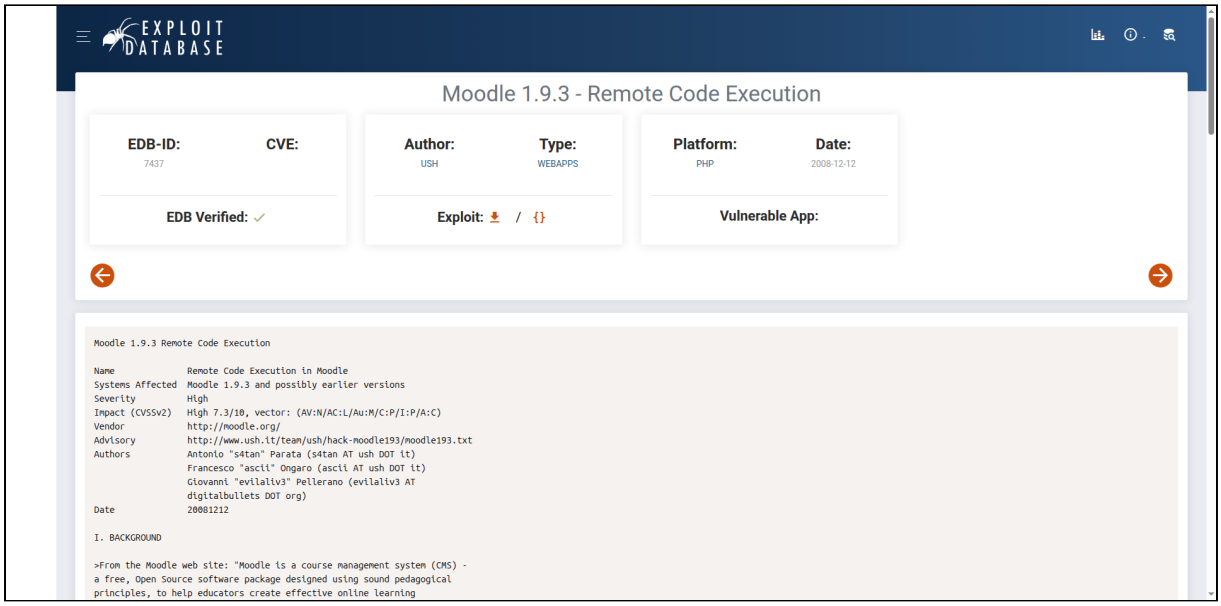
PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

Page Screenshot



Moodle 1.9.3 - Remote Code Execution

EDB-ID:
7437

CVE:

EDB Verified: ✓

Author:
USH

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2008-12-12

Vulnerable App:

```
Moodle 1.9.3 Remote Code Execution

Name              Remote Code Execution in Moodle
Systems Affected  Moodle 1.9.3 and possibly earlier versions
Severity          High
Impact (CVSSv2)   High 7.3/10, vector: (AV:N/AC:L/Au:M/C:P/I:P/A:C)
Vendor            http://moodle.org/
Advisory          http://www.ush.it/team/ush/hack-moodle193/moodle193.txt
Authors           Antonio "s4tan" Parata (s4tan AT ush DOT it)
                  Francesco "ascii" Ongaro (ascii AT ush DOT it)
                  Giovanni "evilaliv3" Pellerano (evilaliv3 AT
                  digitalbullets DOT org)
Date              20081212

I. BACKGROUND

>From the Moodle web site: "Moodle is a course management system (CMS) -
a free, Open Source software package designed using sound pedagogical
principles, to help educators create effective online learning
communities".

II. DESCRIPTION

A Remote Code Execution exists in Moodle 1.9.3.

III. ANALYSIS

- Remote Code Execution (RCE) in texed.php (pathname parameter)

A Remote Code Execution (RCE) vulnerability has been found in
filter/tex/texed.php. In order to exploit this vulnerability
register_globals must be enabled as the "TeX Notation" filter.

All these conditions reduce the impact of the vulnerability, to remark
this fact we have set "multiple authentication" flag in the cvss2 score).

In texed.php we find the following instructions:

--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--

$cmd = tex_filter_get_cmd($pathname, $texexp);
system($cmd, $status);

--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--

Where the function "tex_filter_get_cmd", defined in lib.php, is the
following:

--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--

function tex_filter_get_cmd($pathname, $texexp) {
    $texexp = escapeshellarg($texexp);
    $executable = tex_filter_get_executable(false);

    if ((PHP_OS == "WINNT") || (PHP_OS == "WIN32") || (PHP_OS ==
"Windows")) {
        $executable = str_replace(' ', '^ ', $executable);
        return "$executable ++ -e  \"$pathname\" -- $texexp";

    } else {
        return "\"$executable\" -e \"$pathname\" -- $texexp";
    }
}

--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--8<--

As we can see no check is performed on the "$pathname" parameter neither
in "texed.php" neither in the "tex_filter_get_cmd" function declared in
"lib.php".

Seen this it's possible to exploit this vulnerability to execute
arbitrary commands on the target server. The following urls are proof
of concept for Linux and Windows:

On Linux:
http://www.example.com/moodle/filter/tex/texed.php?formdata=foo&pathname=foo";ls+-l;echo+"

On Windows:
http://www.example.com/moodle/filter/tex/texed.php?formdata=foo&pathname=foo"+||+dir+||+echo+

This RCE is "blind". You'll never see the list dir of the example
because there is no print of the system command output.

IV. DETECTION

Moodle 1.9.3 and possibly earlier versions are vulnerable.

V. WORKAROUND

Proper input validation will fix the vulnerabilities. Actually the
vulnerability is fixed in the Dev tree.

Upgrade to latest development version.

VI. VENDOR RESPONSE

Vendor will not release a new version addressing this vulnerability
since moodle has several different issues with register globals and
the vendor decided to resolve them in a different way for the upcoming
versions.

"At present we are working on changes that will prevent installation when
register globals on. They should be committed later this week. I suppose
we are not going to release 1.9.4 now because register globals issue is
a know problem already."

VII. CVE INFORMATION
```

```
No CVE at this time.

VIII. DISCLOSURE TIMELINE

20080121 Bug discovered
20081111 Initial vendor contact (No Response)
20081811 Second vendor contact (No Response)
20081811 Vendor response
20081212 Advisory released (Fix available only in dev tree)

IX. CREDIT

Antonio "s4tan" Parata, Francesco "ascii" Ongaro and Giovanni
"evilaliv3" Pellerano are credited with the discovery of this
vulnerability.

Antonio "s4tan" Parata
web site: http://www.ictsc.it/
mail: s4tan AT ictsc DOT it, s4tan AT ush DOT it

Francesco "ascii" Ongaro
web site: http://www.ush.it/
mail: ascii AT ush DOT it

Giovanni "evilaliv3" Pellerano
mail: evilaliv3 AT digitalbullets DOT it

X. LEGAL NOTICES

Copyright (c) 2008 Francesco "ascii" Ongaro

Permission is granted for the redistribution of this alert
electronically. It may not be edited in any way without mine express
written consent. If you wish to reprint the whole or any
part of this alert in any other medium other than electronically,
please email me for permission.

Disclaimer: The information in the advisory is believed to be accurate
at the time of publishing based on currently available information. Use
of the information constitutes acceptance for use in an AS IS condition.
There are no warranties with regard to this information. Neither the
author nor the publisher accepts any liability for any direct, indirect,
or consequential loss or damage arising from use of, or reliance on,
this information.

# milw0rm.com [2008-12-12]
```

Tags:

Advisory/Source: Link