sanluan / **PublicCMS** Public

Code · Issues 1 · Pull requests 1 · Discussions · Actions · Security · ...

New issue

Jump to bottom

#59

Closed **chauncyman** opened this issue on Nov 25, 2021 · 8 comments

chauncyman commented on Nov 25, 2021 • edited

PublicCMS v4.0 Value parameter has command execution vulnerability

Vulnerability Type :

command execution

Vulnerability Version :

4.0

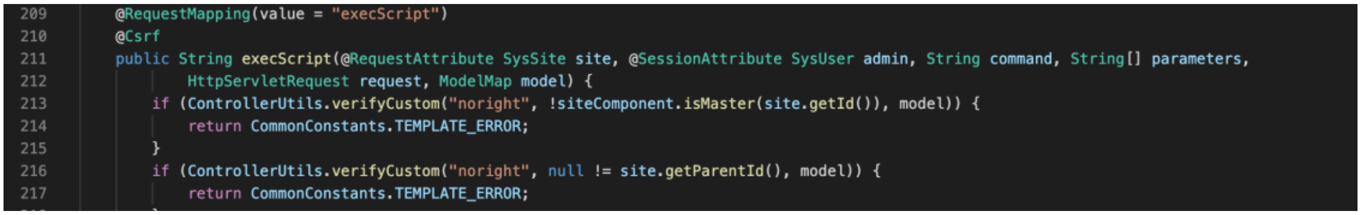
##Vulnerability location：
PublicCMS-4.0.202107.c/publiccms-parent/publiccms-core/src/main/java/com/publiccms/controller/admin/sys/SysSiteAdminController.java:249

Vulnerability Description AND recurrence:

Manual audit of publiccms source code，a command execution vulnerability was discovered

Vulnerable link 1: PublicCMS-4.0.202107.c/publiccms-parent/publiccms-core/src/main/java/com/publiccms/contr
oller/admin/sys/SysSiteAdminController.java:211

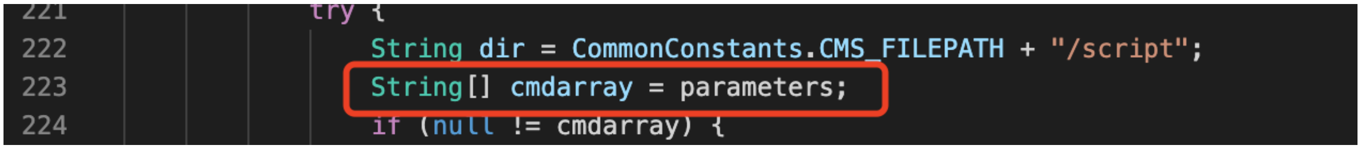
`parameters` is the source of taint, value:<> （ **`parameters` 是污点来源，value:<>** ）



```
209     @RequestMapping(value = "execScript")
210     @Csrf
211     public String execScript(@RequestAttribute SysSite site, @SessionAttribute SysUser admin, String command, String[] parameters,
212             HttpServletRequest request, ModelMap model) {
213         if (ControllerUtils.verifyCustom("noright", !siteComponent.isMaster(site.getId()), model)) {
214             return CommonConstants.TEMPLATE_ERROR;
215         }
216         if (ControllerUtils.verifyCustom("noright", null != site.getParentId(), model)) {
217             return CommonConstants.TEMPLATE_ERROR;
```

Vulnerable link 2：PublicCMS-4.0.202107.c/publiccms-parent/publiccms-core/src/main/java/com/publiccms/controller/admin/sys/SysSiteAdminController.java:223

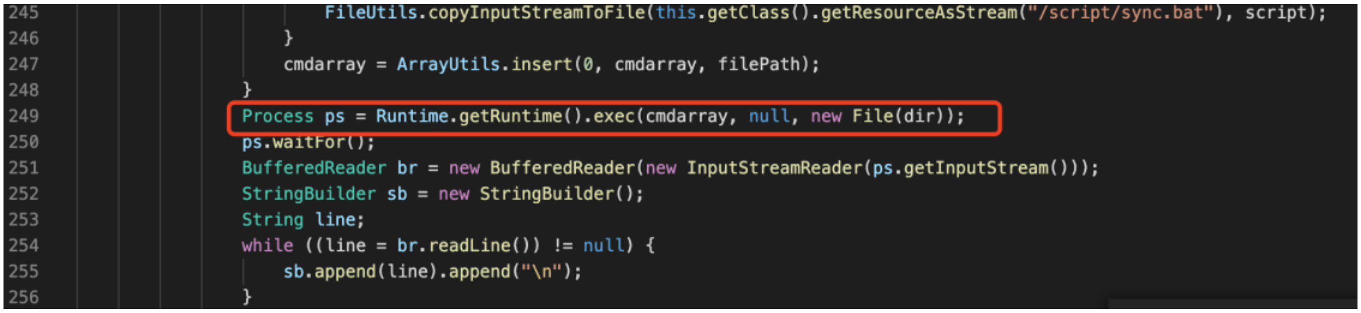
The stain is passed from `parameters` to `cmdarray` , value:<> **（污点从 `parameters` 传递至 `cmdarray` ， value:<>）**



```
221             try {
222                 String dir = CommonConstants.CMS_FILEPATH + "/script";
223                 String[] cmdarray = parameters;
224                 if (null != cmdarray) {
```

Vulnerable link 3：PublicCMS-4.0.202107.c/publiccms-parent/publiccms-core/src/main/java/com/publiccms/contr
oller/admin/sys/SysSiteAdminController.java:249

`RCE` type risk trigger, caused by the input parameter `cmdarray` , value:<> **(`RCE` 类型风险触发，由入参 `cmdarray` 导致，value:<>)**



```
245                         FileUtils.copyInputStreamToFile(this.getClass().getResourceAsStream("/script/sync.bat"), script);
246                     }
247                     cmdarray = ArrayUtils.insert(0, cmdarray, filePath);
248                 }
249                 Process ps = Runtime.getRuntime().exec(cmdarray, null, new File(dir));
250                 ps.waitFor();
251                 BufferedReader br = new BufferedReader(new InputStreamReader(ps.getInputStream()));
252                 StringBuilder sb = new StringBuilder();
253                 String line;
254                 while ((line = br.readLine()) != null) {
255                     sb.append(line).append("\n");
256                 }
```

chauncyman closed this as completed on Nov 25, 2021

chauncyman reopened this on Nov 25, 2021

zrquan commented on Jan 24

这里不是做了限制吗

sanluan closed this as completed on Feb 10

Howsson commented on Mar 10 • edited

不是已经白名单了吗 看这里

zongdeiqianxing commented on Apr 6

这个作者认定不存在的漏洞 也能分配cve嘛？？
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23389

1 similar comment

0neOfU4 commented on Apr 6

这种感觉是某种代码审计工具扫描出来的，应该自己试试再报吧，至少有个利用成功截图比较好

zongdeiqianxing commented on Apr 6

关键是还申请到cve了 就离谱

> 这种感觉是某种代码审计工具扫描出来的，应该自己试试再报吧，至少有个利用成功截图比较好

chauncyman changed the title ~~Arbitrary command execution vulnerability （任意命令执行漏洞）~~ # on Apr 6

0neOfU4 commented on Apr 6

> 关键是还申请到cve了 就离谱
>
> > 这种感觉是某种代码审计工具扫描出来的，应该自己试试再报吧，至少有个利用成功截图比较好

dd行为，就是好奇用的啥工具，类似于codeql吗

shellfeel commented on Oct 20

> > 关键是还申请到cve了 就离谱
> >
> > > 这种感觉是某种代码审计工具扫描出来的，应该自己试试再报吧，至少有个利用成功截图比较好
>
> dd行为，就是好奇用的啥工具，类似于codeql吗

没错就是codeql 😜

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

7 participants