» Issue41304

This issue tracker **has been migrated to GitHub**, and is currently **read-only**.
For more information, **see the GitHub FAQs in the Python's Developer Guide.**

This issue has been migrated to GitHub:
https://github.com/python/cpython/issues/85476

classification

Title:	[CVE-2020-15801] python 38 embed ignore python38._pth file on windows		
Type:	security	**Stage**:	resolved
Components:	Interpreter Core, Windows	**Versions**:	Python 3.10, Python 3.9, Python 3.8, Python 3.7

process

Status:	closed	**Resolution**:	fixed
Dependencies:		**Superseder**:	
Assigned To:		**Nosy List**:	jgirardet, miss-islington, ned.deily, owen.huang, paul.moore, steve.dower, tim.golden, zach.ware
Priority:	normal	**Keywords**:	3.8regression, patch

Created on **2020-07-15 14:41** by **jgirardet**, last changed **2022-04-11 14:59** by **admin**. This issue is now **closed**.

Pull Requests

URL	Status	Linked	Edit
PR 21495	merged	steve.dower, 2020-07-15 19:31	
PR 21497	merged	miss-islington, 2020-07-15 21:57	
PR 21498	merged	miss-islington, 2020-07-15 21:57	
PR 21499	merged	steve.dower, 2020-07-15 21:59	
PR 21521	merged	steve.dower, 2020-07-17 16:34	
PR 21522	merged	miss-islington, 2020-07-17 16:47	
PR 21524	merged	miss-islington, 2020-07-17 16:47	
PR 21523	merged	miss-islington, 2020-07-17 16:48	

Messages (14)

msg373698 - (view) **Author: Jimmy Girardet (jgirardet)** **Date: 2020-07-15 14:41**

```
Hi,
With python embed unziped in `38` directory(python 3.8.4):
```

```
# python38._pth
python38.zip
.
..\\app
# Uncomment to run site.main() automatically
#import site
```

```
PS C:\Users\jimmy\rien\embed> .\38\python.exe -c "import
sys;print(sys.path);import hello"
['', 'C:\\Users\\jimmy\\rien\\embed\\38\\python38.zip',
'C:\\Users\\jimmy\\rien\\embed\\38\\DLLs', 'C:\\Users\\jimmy\\ri
en\\embed\\38\\lib', 'C:\\Users\\jimmy\\rien\\embed\\38']
Traceback (most recent call last):
  File "<string>", line 1, in <module>
ModuleNotFoundError: No module named 'hello'


'\\app' is not added to sys.path. it is under python 3.
```

Note It's working under python 3.7.8

msg373701 - (view) **Author: Jimmy Girardet (jgirardet)** **Date: 2020-07-15 15:32**

replacing python38._pth by python._pth does fix it.

msg373706 - (view) **Author: Steve Dower (steve.dower) *** **Date: 2020-07-15 18:07**

Thanks, this is a regression.

https://github.com/python/cpython/blob/master/PC/getpathp.c#L672 should be inverted, as a zero return value indicates success.

msg373727 - (view) **Author: Steve Dower (steve.dower) *** **Date: 2020-07-15 21:56**

New changeset **936a66094591dc0e67d4a60c170148bb700ec016** by Steve Dower in branch 'master':
~~bpo-41304~~: Ensure python3x._pth is loaded on Windows (**~~GH-21495~~**)
https://github.com/python/cpython/commit/936a66094591dc0e67d4a60c170148bb700ec016

msg373728 - (view) **Author: miss-islington (miss-islington)** **Date: 2020-07-15 22:14**

New changeset **28e93dd2b26c460424acbebd00d8b943abbbea17** by Miss Islington (bot) in branch '3.9':
~~bpo-41304~~: Ensure python3x._pth is loaded on Windows (**~~GH-21495~~**)
https://github.com/python/cpython/commit/28e93dd2b26c460424acbebd00d8b943abbbea17

msg373729 - (view) **Author: miss-islington (miss-islington)** **Date: 2020-07-15 22:15**

New changeset **3b6a8d2455c6897085f4277737b0f9b9a3847c24** by Miss Islington (bot) in branch '3.8':

~~bpo-41304~~: Ensure python3x._pth is loaded on Windows (~~GH-21495~~)
https://github.com/python/cpython/commit/3b6a8d2455c6897085f4277737b0f9b9a3847c24

msg373731 - (view) **Author: Ned Deily (ned.deily) *** **Date: 2020-07-15 22:24**

New changeset 4bfcffe16e9742c154f54ae96b5b36903500abaa by Steve Dower in branch '3.7':
~~bpo-41304~~: Ensure python3x._pth is loaded on Windows (~~GH-21495~~) (~~#21499~~)
https://github.com/python/cpython/commit/4bfcffe16e9742c154f54ae96b5b36903500abaa

msg373756 - (view) **Author: Steve Dower (steve.dower) *** **Date: 2020-07-16 17:08**

For clarity, this was caused by the fix for ~~issue29778~~, and was only released in 3.8.4 and 3.9.0b4. No other versions had a release before the fix was merged.

msg373836 - (view) **Author: Steve Dower (steve.dower) *** **Date: 2020-07-17 16:29**

This is now assigned CVE-2020-15801

msg373837 - (view) **Author: Steve Dower (steve.dower) *** **Date: 2020-07-17 16:54**

New changeset a16ac4e43c8ed15bf2fca52df3a0a5de26ad2705 by Miss Islington (bot) in branch '3.9':
~~bpo-41304~~: Update NEWS to include CVE-2020-15801 reference (~~GH-21521~~)
https://github.com/python/cpython/commit/a16ac4e43c8ed15bf2fca52df3a0a5de26ad2705

msg373838 - (view) **Author: Steve Dower (steve.dower) *** **Date: 2020-07-17 16:54**

New changeset 79ed1a53fa44a1b74e3c24c9d5f698abd9610921 by Miss Islington (bot) in branch '3.8':
~~bpo-41304~~: Update NEWS to include CVE-2020-15801 reference (~~GH-21521~~)
https://github.com/python/cpython/commit/79ed1a53fa44a1b74e3c24c9d5f698abd9610921

msg373891 - (view) **Author: Ned Deily (ned.deily) *** **Date: 2020-07-18 09:01**

New changeset eb0d255ffe002412bb937e1bde61225e5431da5e by Miss Islington (bot) in branch '3.7':
~~bpo-41304~~: Update NEWS to include CVE-2020-15801 reference (~~GH-21521~~) (~~GH-21524~~)
https://github.com/python/cpython/commit/eb0d255ffe002412bb937e1bde61225e5431da5e

msg374912 - (view) **Author: huangtaizhuo (owen.huang)** **Date: 2020-08-06 02:40**

hi, since the affected system is not clearly stated on the NVD, I'd like to confirm with you that:

Does the CVE-2020-15801 vulnerability affect only the Windows OS?

thanks a lot!

msg374942 - (view) **Author: Steve Dower (steve.dower) *** **Date: 2020-08-06 16:10**

```
Yes, it only affects Windows OS.

On all other platforms, the python38._pth file is _always_ ignored. We have not
implemented this support for those platforms.
```

History

Date	User	Action	Args
2022-04-11 14:59:33	admin	set	github: 85476
2020-08-06 16:10:28	steve.dower	set	messages: + **msg374942**
2020-08-06 02:40:05	owen.huang	set	nosy: + **owen.huang** messages: + **msg374912**
2020-07-18 09:01:05	ned.deily	set	messages: + **msg373891**
2020-07-17 16:54:14	steve.dower	set	messages: + **msg373838**
2020-07-17 16:54:03	steve.dower	set	messages: + **msg373837**
2020-07-17 16:48:01	miss-islington	set	pull_requests: + **pull_request20661**
2020-07-17 16:47:55	miss-islington	set	pull_requests: + **pull_request20660**
2020-07-17 16:47:47	miss-islington	set	pull_requests: + **pull_request20659**
2020-07-17 16:34:39	steve.dower	set	pull_requests: + **pull_request20658**
2020-07-17 16:29:34	steve.dower	set	messages: + **msg373836** title: python 38 embed ignore python38._pth file on windows -> [CVE-2020-15801] python 38 embed ignore python38._pth file on windows
2020-07-16 17:08:16	steve.dower	set	status: open -> closed resolution: fixed messages: + **msg373756** stage: patch review -> resolved
2020-07-15 22:24:59	ned.deily	set	nosy: + **ned.deily** messages: + **msg373731**
2020-07-15 22:15:45	miss-islington	set	messages: + **msg373729**
2020-07-15 22:14:55	miss-islington	set	messages: + **msg373728**
2020-07-15 21:59:59	steve.dower	set	pull_requests: + **pull_request20641**
2020-07-15 21:57:14	miss-islington	set	pull_requests: + **pull_request20640**
2020-07-15 21:57:05	miss-islington	set	nosy: + **miss-islington** pull_requests: + **pull_request20639**
2020-07-15 21:56:55	steve.dower	set	messages: + **msg373727**
2020-07-15 19:31:43	steve.dower	set	keywords: + **patch** stage: test needed -> patch review

			pull_requests: + **pull_request20637**
2020-07-15 18:08:21	steve.dower	set	type: security stage: test needed
2020-07-15 18:07:59	steve.dower	set	keywords: + **3.8regression** messages: + **msg373706** versions: + Python 3.7, Python 3.9, Python 3.10
2020-07-15 15:39:45	xtreak	set	nosy: + **paul.moore**, **tim.golden**, **zach.ware**, **steve.dower** components: + Windows
2020-07-15 15:32:39	jgirardet	set	messages: + **msg373701**
2020-07-15 14:41:43	jgirardet	set	title: python 38 embed ignore python38._pth file -> python 38 embed ignore python38._pth file on windows
2020-07-15 14:41:17	jgirardet	create	