» Issue43285



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/87451

classification

Title: ftplib should not use the host from the PASV response	
Type: security	**Stage**: resolved
Components: Library (Lib)	**Versions**: Python 3.7, Python 3.6

process

Status: closed	**Resolution**: fixed
Dependencies:	**Superseder**:
Assigned To:	**Nosy List**: giampaolo.rodola, gregory.p.smith, miss-islington, ned.deily, ricexdream
Priority: release blocker	**Keywords**: patch

Created on **2021-02-21 11:49** by **ricexdream**, last changed **2022-04-11 14:59** by **admin**. This issue is now **closed**.

Pull Requests

URL	Status	Linked	Edit
PR 24838	merged	gregory.p.smith, 2021-03-13 11:54	
PR 24880	merged	miss-islington, 2021-03-15 18:39	
PR 24881	merged	gregory.p.smith, 2021-03-15 18:49	
PR 24882	merged	miss-islington, 2021-03-15 19:05	
PR 24883	merged	miss-islington, 2021-03-15 19:05	
PR 24886	closed	gregory.p.smith, 2021-03-16 04:02	
PR 24887	closed	gregory.p.smith, 2021-03-16 04:02	
PR 24888	merged	gregory.p.smith, 2021-03-16 04:11	
PR 24889	merged	gregory.p.smith, 2021-03-16 04:13	

Messages (16)

msg387455 - (view) **Author: confd0 (ricexdream)** **Date: 2021-02-21 11:49**

Last year, curl had a security update for CVE-2020-8284. more info, see
https://hackerone.com/reports/1040166

The problem is ftp client trust the host from PASV response by default, A malicious server can trick ftp client into connecting
back to a given IP address and port. This may make ftp client scan ports and extract service banner from private newwork.

After test and read ftplib module(**https://github.com/python/cpython/blob/63298930fb531ba2bb4f23bc3b915dbf1e17e9e1/Lib/ftplib.py#L346**), I found ftplib has the same problem.

msg388267 - (view) **Author: confd0 (ricexdream)** **Date: 2021-03-08 13:42**

Any response here? If you need more information let me know.

msg388602 - (view) **Author: Gregory P. Smith (gregory.p.smith) *** **Date: 2021-03-13 10:30**

Indeed, the `host` on that line there should just be ignored with the IP address of the original data connection used in its place.

Your **https://hackerone.com/reports/1040166** link provides plenty of information and likes to prior art mitigations other ftp clients including Firefox and Chrome well over a decade ago.

msg388610 - (view) **Author: Gregory P. Smith (gregory.p.smith) *** **Date: 2021-03-13 12:03**

I'm not interested in chasing down a CVE for this myself. If anyone wants to jump through the hoops to obtain one, the text used for curl in the hackerone link is likely a good guide.

My PR includes a way for people to opt-out of the secure behavior (why would anyone ever want that?) by setting the use_untrusted_server_pasv_ipv4_addr attribute to True on their ftplib.FTP instance. Setting that attribute on a server lacking this fix is a no-op, making it safe to add to code running on any version.

This is an embarrassingly old widespread common issue in a large number of ftp clients. Even the 1998 IPv6 RFC **https://tools.ietf.org/html/rfc2428** indirectly acknowledges its existence by disallowing the new EPSV command that replaces PASV from returning anything other than the port number while leaving fields for the other values present but empty...

msg388757 - (view) **Author: Gregory P. Smith (gregory.p.smith) *** **Date: 2021-03-15 18:39**

New changeset **0ab152c6b5d95caa2dc1a30fa96e10258b5f188e** by Gregory P. Smith in branch 'master':
~~**bpo-43285**~~ Make ftplib not trust the PASV response. (~~**GH-24838**~~)
https://github.com/python/cpython/commit/0ab152c6b5d95caa2dc1a30fa96e10258b5f188e

msg388761 - (view) **Author: miss-islington (miss-islington)** **Date: 2021-03-15 19:02**

New changeset **7dcb4baa4f0fde3aef5122a8e9f6a41853ec9335** by Miss Islington (bot) in branch '3.9':
~~**bpo-43285**~~ Make ftplib not trust the PASV response. (~~**GH-24838**~~)
https://github.com/python/cpython/commit/7dcb4baa4f0fde3aef5122a8e9f6a41853ec9335

msg388762 - (view) **Author: Gregory P. Smith (gregory.p.smith) *** **Date: 2021-03-15 19:04**

New changeset **664d1d16274b47eea6ec92572e1ebf3939a6fa0c** by Gregory P. Smith in branch '3.8':
[3.8] ~~**bpo-43285**~~ Make ftplib not trust the PASV response. (~~**GH-24838**~~) (~~**GH-24881**~~)
https://github.com/python/cpython/commit/664d1d16274b47eea6ec92572e1ebf3939a6fa0c

msg388763 - (view) **Author: Gregory P. Smith (gregory.p.smith) *** **Date: 2021-03-15 19:08**

3.7 and 3.6 backport PRs created and assigned to release manager Ned for merging.

msg388768 - (view) **Author: Ned Deily (ned.deily) *** **Date: 2021-03-15 19:38**

@gps, What about ftplib doc changes and What's new entries for this change in behavior?

msg388777 - (view) **Author: Gregory P. Smith (gregory.p.smith) *** **Date: 2021-03-15 21:56**

A What's New entry is a good idea. I'll make one and add it to those backport PRs. (reopened to remind me of that)

ftplib docs... I don't actually want to document the attribute that people can set for the old behavior beyond the notes in NEWS or What's New. It is something I anticipate nobody in the world ever actually setting so I'd rather not imply that anyone even should by giving it more prominent doc space.

Other things that have fixed this repeated bug in their program that supports ftp over the years have not added an opt-out as far as I could tell in my quick searching.

msg388812 - (view) **Author: Gregory P. Smith (gregory.p.smith) *** **Date: 2021-03-16 04:38**

New changeset **d0312cece9ce89d783687ff6dddaae6495e19fcf** by Gregory P. Smith in branch '3.9':
[3.9] ~~**bpo-43285**~~: Add a What's New entry for 3.9.3. (~~**GH-24888**~~)
https://github.com/python/cpython/commit/d0312cece9ce89d783687ff6dddaae6495e19fcf

msg388813 - (view) **Author: Gregory P. Smith (gregory.p.smith) *** **Date: 2021-03-16 04:38**

New changeset **9eda0dfff2884bf9272f37d4151ef2335f55066f** by Gregory P. Smith in branch '3.8':
[3.8] ~~**bpo-43285**~~: Whats New entry for 3.8.9. (~~**GH-24889**~~)
https://github.com/python/cpython/commit/9eda0dfff2884bf9272f37d4151ef2335f55066f

msg388815 - (view) **Author: Gregory P. Smith (gregory.p.smith) *** **Date: 2021-03-16 04:39**

3.7 and 3.6 PRs updated to include a What's New entry.

msg388882 - (view) **Author: Ned Deily (ned.deily) *** **Date: 2021-03-16 21:08**

New changeset **4134f154ae2f621f25c5d698cc0f1748035a1b88** by Miss Islington (bot) in branch '3.6':
[3.6] ~~**bpo-43285**~~ Make ftplib not trust the PASV response. (~~**GH-24838**~~) (~~**GH-24881**~~) (~~**GH-24882**~~)
https://github.com/python/cpython/commit/4134f154ae2f621f25c5d698cc0f1748035a1b88

msg388885 - (view) **Author: Ned Deily (ned.deily) *** **Date: 2021-03-16 21:20**

New changeset **79373951b3eab585d42e0f0ab83718cbe1d0ee33** by Miss Islington (bot) in branch '3.7':
[3.7] ~~**bpo-43285**~~ Make ftplib not trust the PASV response. (~~**GH-24838**~~) (~~**GH-24881**~~) (~~**GH-24883**~~)
https://github.com/python/cpython/commit/79373951b3eab585d42e0f0ab83718cbe1d0ee33

msg388891 - (view) **Author: Ned Deily (ned.deily) *** **Date: 2021-03-16 21:54**

Thanks for the PRs and the What's New entries.

History

Date	User	Action	Args
2022-04-11 14:59:41	admin	set	github: 87451
2021-03-16 21:54:25	ned.deily	set	status: open -> closed assignee: **ned.deily** -> messages: + **msg388891** stage: patch review -> resolved
2021-03-16 21:20:03	ned.deily	set	messages: + **msg388885**
2021-03-16 21:08:37	ned.deily	set	messages: + **msg388882**
2021-03-16 04:39:07	gregory.p.smith	set	priority: normal -> release blocker assignee: **gregory.p.smith** -> **ned.deily** messages: + **msg388815** versions: - Python 3.8, Python 3.9, Python 3.10
2021-03-16 04:38:31	gregory.p.smith	set	messages: + **msg388813**
2021-03-16 04:38:06	gregory.p.smith	set	messages: + **msg388812**
2021-03-16 04:13:37	gregory.p.smith	set	pull_requests: + **pull_request23650**
2021-03-16 04:11:11	gregory.p.smith	set	pull_requests: + **pull_request23649**
2021-03-16 04:02:51	gregory.p.smith	set	pull_requests: + **pull_request23648**
2021-03-16 04:02:37	gregory.p.smith	set	stage: commit review -> patch review pull_requests: + **pull_request23647**
2021-03-15 21:56:22	gregory.p.smith	set	status: closed -> open messages: + **msg388777**
2021-03-15 19:38:04	ned.deily	set	messages: + **msg388768**
2021-03-15 19:08:47	gregory.p.smith	set	status: open -> closed nosy: + **ned.deily** messages: + **msg388763** resolution: fixed stage: patch review -> commit review

2021-03-15 19:05:35	miss-islington	set	pull_requests: + **pull_request23641**
2021-03-15 19:05:03	miss-islington	set	pull_requests: + **pull_request23640**
2021-03-15 19:04:56	gregory.p.smith	set	messages: + **msg388762**
2021-03-15 19:02:53	miss-islington	set	messages: + **msg388761**
2021-03-15 18:49:54	gregory.p.smith	set	pull_requests: + **pull_request23639**
2021-03-15 18:39:41	miss-islington	set	nosy: + **miss-islington** pull_requests: + **pull_request23638**
2021-03-15 18:39:38	gregory.p.smith	set	messages: + **msg388757**
2021-03-13 12:04:37	gregory.p.smith	set	title: ftplib use host from PASV response -> ftplib should not use the host from the PASV response
2021-03-13 12:03:41	gregory.p.smith	set	messages: + **msg388610**
2021-03-13 11:54:48	gregory.p.smith	set	keywords: + **patch** stage: needs patch -> patch review pull_requests: + **pull_request23603**
2021-03-13 10:30:43	gregory.p.smith	set	versions: + Python 3.6, Python 3.7, Python 3.8, Python 3.10 nosy: + **gregory.p.smith** messages: + **msg388602** assignee: **gregory.p.smith** stage: needs patch
2021-03-08 13:42:54	ricexdream	set	messages: + **msg388267**
2021-02-21 15:36:22	shihai1991	set	nosy: + **giampaolo.rodola**
2021-02-21 11:49:34	ricexdream	create	