» Issue34623



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/78804

classification

Title: _elementtree.c doesn't call XML_SetHashSalt()	
Type: security	**Stage**: resolved
Components: XML	**Versions**: Python 3.4, Python 3.5

process

Status: closed	**Resolution**: fixed
Dependencies:	**Superseder**:
Assigned To: larry	**Nosy List**: benjamin.peterson, christian.heimes, cstratak, larry, mcepl, miss-islington, ned.deily, vstinner
Priority: release blocker	**Keywords**: patch

Created on **2018-09-10 22:47** by **christian.heimes**, last changed **2022-04-11 14:59** by **admin**. This issue is now **closed**.

Files

File name	Uploaded	Description	Edit
CVE-2018-14647_XML_SetHashSalt-in_elementtree.patch	mcepl, 2019-01-25 21:09		

Pull Requests

URL	Status	Linked	Edit
PR 9146	merged	christian.heimes, 2018-09-10 23:07	
PR 9392	merged	miss-islington, 2018-09-18 12:39	
PR 9393	merged	miss-islington, 2018-09-18 12:39	
PR 9394	merged	christian.heimes, 2018-09-18 12:45	
PR 9482	merged	christian.heimes, 2018-09-21 20:51	
PR 9488	merged	miss-islington, 2018-09-22 04:42	
PR 9489	merged	miss-islington, 2018-09-22 04:42	
PR 9490	merged	miss-islington, 2018-09-22 04:43	
PR 9933	merged	cstratak, 2018-10-17 16:25	

PR 9953 merged cstratak, 2018-10-18 14:59

Messages (20)

msg324954 - (view) **Author: Christian Heimes (christian.heimes) *** **Date: 2018-09-10 22:47**

The pyexpat module calls XML_SetHashSalt(self->itself, (unsigned long)_Py_HashSecret.expat.hashsalt) to initialize the salt for hash randomization of the XML_Parser struct. The _elementree C accelerator doesn't call XML_SetHashSalt().

It's not a security issue with recent versions of libexpat. The library initializes the salt from a good entry source by default.

msg324961 - (view) **Author: Benjamin Peterson (benjamin.peterson) *** **Date: 2018-09-10 23:48**

Note we compile expat with -DXML_POOR_ENTROPY on the assumption that Python always initializes the entropy itself.

msg324963 - (view) **Author: STINNER Victor (vstinner) *** **Date: 2018-09-11 00:09**

> Note we compile expat with -DXML_POOR_ENTROPY on the assumption that Python always initializes the entropy itself.

Oh. I forgot this thing. So it seems like we have to backport this change to 2.7, 3.6 and newer versions.

What about Python 3.4 and 3.5? Python 3.5 has a copy of libexpat 2.2.0, but setup.py doesn't build expat with XML_POOR_ENTROPY=1.

msg324966 - (view) **Author: Christian Heimes (christian.heimes) *** **Date: 2018-09-11 00:38**

Dang, it's a security bug after all. :(

3.5 has 2.2.4, so it's fine. 2.2.2 had a bug in salt initialization.

msg325633 - (view) **Author: miss-islington (miss-islington)** **Date: 2018-09-18 12:39**

New changeset **cb5778f00ce48631c7140f33ba242496aaf7102b** by Miss Islington (bot) (Christian Heimes) in branch 'master':
~~**bpo-34623**~~: Use XML_SetHashSalt in _elementtree (**GH-9146**)
https://github.com/python/cpython/commit/cb5778f00ce48631c7140f33ba242496aaf7102b

msg325634 - (view) **Author: Christian Heimes (christian.heimes) *** **Date: 2018-09-18 12:40**

Since it's a security fix, the change should land in 3.4 and 3.5, too.

msg325636 - (view) **Author: miss-islington (miss-islington)** **Date: 2018-09-18 13:11**

New changeset **470a435f3b42c9be5fdb7f7b04f3df5663ba7305** by Miss Islington (bot) in branch '3.7':
~~**bpo-34623**~~: Use XML_SetHashSalt in _elementtree (**GH-9146**)
https://github.com/python/cpython/commit/470a435f3b42c9be5fdb7f7b04f3df5663ba7305

msg325637 - (view) **Author: miss-islington (miss-islington)** **Date: 2018-09-18 13:13**

New changeset **18b20bad75b4ff0486940fba4ec680e96e70f3a2** by Miss Islington (bot) (Christian Heimes) in branch '2.7':
[2.7] ~~**bpo-34623**~~: Use XML_SetHashSalt in _elementtree (**GH-9146**) (~~**GH-9394**~~)
https://github.com/python/cpython/commit/18b20bad75b4ff0486940fba4ec680e96e70f3a2

msg325638 - (view) **Author: miss-islington (miss-islington)** **Date: 2018-09-18 13:14**

New changeset **f7666e828cc3d5873136473ea36ba2013d624fa1** by Miss Islington (bot) in branch '3.6':
~~**bpo-34623**~~: Use XML_SetHashSalt in _elementtree (**GH-9146**)
https://github.com/python/cpython/commit/f7666e828cc3d5873136473ea36ba2013d624fa1

msg325966 - (view) **Author: Christian Heimes (christian.heimes) *** **Date: 2018-09-21 06:38**

The bug affects multiple platforms. libexpat's expat.h uses slightly different autoconf macro names than pyconfig.h. Therefore only platforms that have either HAVE_GETRANDOM or _WIN32 defined, use a proper CSPRNG to seed the hash salt.

Since HAVE_SYSCALL_GETRANDOM, HAVE_ARC4RANDOM_BUF, HAVE_ARC4RANDOM, or XML_DEV_URANDOM are never defined by Python's pyconfig.h, older Linux platforms, any BSD, and any other Unix platform with /dev/urandom fall back to a weak Mersenne Twister-like RNG with gettimeofday().tv_usec and getpid() as seed.

msg325967 - (view) **Author: Christian Heimes (christian.heimes) *** **Date: 2018-09-21 06:47**

I have contected Red Hat product security to request a CVE for the issue.

msg326019 - (view) **Author: Christian Heimes (christian.heimes) *** **Date: 2018-09-21 19:16**

CVE-2018-14647 was assigned to this issue.

msg326069 - (view) **Author: miss-islington (miss-islington)** **Date: 2018-09-22 04:42**

New changeset **026337a7101369297c8083047d2f3c6fc9dd1e2b** by Miss Islington (bot) (Christian Heimes) in branch 'master':
~~**bpo-34623**~~: Mention CVE-2018-14647 in news entry (~~**GH-9482**~~)
https://github.com/python/cpython/commit/026337a7101369297c8083047d2f3c6fc9dd1e2b

msg326071 - (view) **Author: miss-islington (miss-islington)** **Date: 2018-09-22 04:57**

New changeset **10be1d3f802b874914b2a13eb41407c7a582d9b3** by Miss Islington (bot) in branch '2.7':
[2.7] ~~**bpo-34623**~~: Mention CVE-2018-14647 in news entry (~~**GH-9482**~~) (~~**GH-9490**~~)
https://github.com/python/cpython/commit/10be1d3f802b874914b2a13eb41407c7a582d9b3

msg326072 - (view) **Author: miss-islington (miss-islington)** **Date: 2018-09-22 04:57**

New changeset **d1b336e530472f316b1d164d04626724c83b16d7** by Miss Islington (bot) in branch '3.6':
[3.6] ~~**bpo-34623**~~: Mention CVE-2018-14647 in news entry (~~**GH-9482**~~) (~~**GH-9489**~~)
https://github.com/python/cpython/commit/d1b336e530472f316b1d164d04626724c83b16d7

msg326073 - (view) **Author: miss-islington (miss-islington)** **Date: 2018-09-22 04:57**

New changeset **5c3d8b2efda1b99abe09ad925f366c5695bd66fb** by Miss Islington (bot) in branch '3.7':
[3.7] ~~**bpo-34623**~~: Mention CVE-2018-14647 in news entry (~~**GH-9482**~~) (~~**GH-9488**~~)
https://github.com/python/cpython/commit/5c3d8b2efda1b99abe09ad925f366c5695bd66fb

msg327758 - (view) **Author: Charalampos Stratakis (cstratak) *** **Date: 2018-10-15 14:10**

Will this change be backported to 3.5 and 3.4? It applied cleanly on both however on 3.4 there is a test failure:

```
======================================================================
ERROR: test_del_attribute (test.test_xml_etree_c.MiscTests)
----------------------------------------------------------------------
Traceback (most recent call last):
  File "/builddir/build/BUILD/Python-3.4.9/Lib/test/test_xml_etree_c.py", line 26, in test_del_attribute
    element = cET.Element('tag')
AttributeError: 'NoneType' object has no attribute 'Element'
----------------------------------------------------------------------
```

msg334369 - (view) **Author: Matej Cepl (mcepl) *** **Date: 2019-01-25 21:09**

> Will this change be backported to 3.5 and 3.4? It applied cleanly on both however on 3.4 there is a test failure:

It actually haven't applied cleanly to me on Python 3.4.6 (SLE-12 package). Apparently self->parser has to be changed into self_xp->parser. Then all tests passed for me.

If any Linux maintainer wants to take this patch.

msg336551 - (view) **Author: Larry Hastings (larry) *** **Date: 2019-02-25 21:02**

New changeset **d16eaf36795da48b930b80b20d3805bc27820712** by larryhastings (stratakis) in branch '3.4':
[3.4] ~~**bpo-34623**~~: Use XML_SetHashSalt in _elementtree (~~**#9953**~~)
https://github.com/python/cpython/commit/d16eaf36795da48b930b80b20d3805bc27820712

msg336552 - (view) **Author: Larry Hastings (larry) *** **Date: 2019-02-25 21:04**

New changeset **41b48e71ac8a71f56694b548f118bd20ce203410** by larryhastings (stratakis) in branch '3.5':
[3.5] ~~**bpo-34623**~~: Use XML_SetHashSalt in _elementtree (~~**#9933**~~)
https://github.com/python/cpython/commit/41b48e71ac8a71f56694b548f118bd20ce203410

History

Date	User	Action	Args
2022-04-11 14:59:05	admin	set	github: 78804
2019-05-10 18:10:05	ned.deily	set	messages: - **msg342101**
2019-05-10 17:36:39	ned.deily	set	nosy: + **ned.deily** messages: + **msg342101**
2019-03-01 07:38:24	larry	set	status: open -> closed resolution: fixed

		stage: patch review -> resolved
2019-02-25 21:04:12	larry	set	messages: + **msg336552**
2019-02-25 21:02:19	larry	set	messages: + **msg336551**
2019-01-25 21:09:57	mcepl	set	files: + **CVE-2018-14647_XML_SetHashSalt-in_elementtree.patch** nosy: + **mcepl** messages: + **msg334369**
2018-10-18 15:22:20	serhiy.storchaka	set	priority: normal -> release blocker assignee: **larry** nosy: + **larry** versions: - Python 2.7, Python 3.6, Python 3.7, Python 3.8
2018-10-18 14:59:05	cstratak	set	pull_requests: + **pull_request9301**
2018-10-17 16:25:33	cstratak	set	pull_requests: + **pull_request9284**
2018-10-15 14:10:45	cstratak	set	nosy: + **cstratak** messages: + **msg327758**
2018-09-22 04:57:49	miss-islington	set	messages: + **msg326073**
2018-09-22 04:57:31	miss-islington	set	messages: + **msg326072**
2018-09-22 04:57:05	miss-islington	set	messages: + **msg326071**
2018-09-22 04:43:05	miss-islington	set	pull_requests: + **pull_request8900**
2018-09-22 04:42:54	miss-islington	set	pull_requests: + **pull_request8899**
2018-09-22 04:42:46	miss-islington	set	pull_requests: + **pull_request8898**
2018-09-22 04:42:33	miss-islington	set	messages: + **msg326069**
2018-09-21 20:51:57	christian.heimes	set	pull_requests: + **pull_request8892**
2018-09-21 19:16:50	christian.heimes	set	messages: + **msg326019**
2018-09-21 06:47:30	christian.heimes	set	messages: + **msg325967**
2018-09-21 06:38:05	christian.heimes	set	messages: + **msg325966**
2018-09-18 13:14:18	miss-islington	set	messages: + **msg325638**
2018-09-18 13:13:12	miss-islington	set	messages: + **msg325637**
2018-09-18 13:11:13	miss-islington	set	messages: + **msg325636**
2018-09-18 12:45:06	christian.heimes	set	pull_requests: + **pull_request8818**
2018-09-18 12:40:28	christian.heimes	set	messages: + **msg325634** versions: + Python 2.7, Python 3.4, Python 3.5
2018-09-18 12:39:20	miss-islington	set	pull_requests: + **pull_request8817**
2018-09-18 12:39:12	miss-islington	set	pull_requests: + **pull_request8816**
2018-09-18 12:39:03	miss-islington	set	nosy: + **miss-islington** messages: + **msg325633**
2018-09-11 00:38:52	christian.heimes	set	type: behavior -> security messages: + **msg324966** versions: + Python 3.6, Python 3.7
2018-09-11 00:09:37	vstinner	set	nosy: + **vstinner** messages: + **msg324963**
2018-09-10 23:48:17	benjamin.peterson	set	nosy: + **benjamin.peterson** messages: + **msg324961**
2018-09-10 23:07:57	christian.heimes	set	keywords: + **patch** stage: patch review pull_requests: + **pull_request8594**
2018-09-10 22:47:44	christian.heimes	create	