classification

Title: [security][CVE-2021-3177] ctypes double representation BoF	
Type: security	**Stage**: resolved
Components: ctypes	**Versions**: Python 3.10, Python 3.9, Python 3.8, Python 3.7, Python 3.6

process

Status: closed	**Resolution**: fixed
Dependencies:	**Superseder**:
Assigned To:	**Nosy List**: Alexander Riccio, JordyZomer, benjamin.peterson, christian.heimes, milanjugessur1404, miss-islington, vstinner
Priority: high	**Keywords**: patch, security_issue

Created on **2021-01-16 08:03** by **JordyZomer**, last changed **2022-04-11 14:59** by **admin**. This issue is now **closed**.

Pull Requests

URL	Status	Linked	Edit
PR 24239	merged	benjamin.peterson, 2021-01-18 15:29	
PR 24247	merged	miss-islington, 2021-01-18 20:47	
PR 24248	merged	miss-islington, 2021-01-18 20:47	
PR 24249	merged	benjamin.peterson, 2021-01-18 20:49	
PR 24250	merged	benjamin.peterson, 2021-01-18 20:51	

Messages (11)

msg385136 - (view) **Author: Jordy Zomer (JordyZomer)** **Date: 2021-01-16 08:03**

```
Hi,

There's a buffer overflow in the PyCArg_repr() function in _ctypes/callproc.c.

The buffer overflow happens due to not checking the length of th sprintf() function on line:

    case 'd':
        sprintf(buffer, "<cparam '%c' (%f)>",
            self->tag, self->value.d);
        break;

Because we control self->value.d we could make it copy _extreme_ values. For example we could make it copy 1e300 which would be a 1
with 300 zero's  to overflow the buffer.

This could potentially cause RCE when a user allows untrusted input in these functions.

A minimal PoC:

>>> from ctypes import *
>>> c_double.from_param(1e300)
*** buffer overflow detected ***: terminated
Aborted


I recommend __always__ controlling how much you copy so I'd use snprintf with a size argument instead.

Best Regards,

Jordy Zomer
```

msg385226 - (view) **Author: Benjamin Peterson (benjamin.peterson) *** **Date: 2021-01-18 20:47**

New changeset **916610ef90a0d0761f08747f7b0905541f0977c7** by Benjamin Peterson in branch 'master':
closes ~~**bpo-42938**~~: Replace snprintf with Python unicode formatting in ctypes param reprs. (24239)
https://github.com/python/cpython/commit/916610ef90a0d0761f08747f7b0905541f0977c7

msg385229 - (view) **Author: Benjamin Peterson (benjamin.peterson) *** **Date: 2021-01-18 21:11**

New changeset **34df10a9a16b38d54421eeeaf73ec89828563be7** by Benjamin Peterson in branch '3.6':
[3.6] closes ~~**bpo-42938**~~: Replace snprintf with Python unicode formatting in ctypes param reprs. (~~**GH-24250**~~)
https://github.com/python/cpython/commit/34df10a9a16b38d54421eeeaf73ec89828563be7

msg385231 - (view) **Author: Benjamin Peterson (benjamin.peterson) *** **Date: 2021-01-18 21:24**

New changeset **d9b8f138b7df3b455b54653ca59f491b4840d6fa** by Benjamin Peterson in branch '3.7':
[3.7] closes ~~**bpo-42938**~~: Replace snprintf with Python unicode formatting in ctypes param reprs. (~~**GH-24249**~~)
https://github.com/python/cpython/commit/d9b8f138b7df3b455b54653ca59f491b4840d6fa

msg385233 - (view) Author: Benjamin Peterson (benjamin.peterson) * Date: 2021-01-18 21:28

New changeset **ece5dfd403dac211f8d3c72701fe7ba7b7aa5b5f** by Miss Islington (bot) in branch '3.8':
closes ~~**bpo-42930**~~: Replace snprintf with Python unicode formatting in ctypes param reprs. (~~**GH-24240**~~)
https://github.com/python/cpython/commit/ece5dfd403dac211f8d3c72701fe7ba7b7aa5b5f

msg385234 - (view) Author: Benjamin Peterson (benjamin.peterson) * Date: 2021-01-18 21:29

New changeset **c347cbe694743cee120457aa6626712f7799a932** by Miss Islington (bot) in branch '3.9':
closes ~~**bpo-42930**~~: Replace snprintf with Python unicode formatting in ctypes param reprs. (~~**GH-24247**~~)
https://github.com/python/cpython/commit/c347cbe694743cee120457aa6626712f7799a932

msg385236 - (view) Author: STINNER Victor (vstinner) * Date: 2021-01-18 22:29

FYI I created **https://python-security.readthedocs.io/vuln/ctypes-buffer-overflow-pycarg_repr.html** to track fixes of this issue.

msg387194 - (view) Author: STINNER Victor (vstinner) * Date: 2021-02-17 22:34

CVE-2021-3177 has been assigned to this issue:
* **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3177**
* **https://access.redhat.com/security/cve/cve-2021-3177**

msg387535 - (view) Author: Alexander Riccio (Alexander Riccio) * Date: 2021-02-22 19:09

Petition to remove all uses of the unchecked string handling functions from CPython?

Sidenote: if C4996 was on, this would be a warning.

msg387536 - (view) Author: Christian Heimes (christian.heimes) * Date: 2021-02-22 19:18

Alexander, this bug report is closed. Could you please open a new request and explain your proposal?

msg387537 - (view) Author: Alexander Riccio (Alexander Riccio) * Date: 2021-02-22 19:27

Yes, I definitely should. I work on **https://bugs.python.org/issue25878** sometimes, which encompasses this.

History

Date	User	Action	Args
2022-04-11 14:59:40	admin	set	github: 87104
2021-03-29 12:32:06	vstinner	set	messages: - **msg389639**
2021-03-29 12:32:05	vstinner	set	messages: - **msg389638**
2021-03-28 17:57:58	milanjugessur1404	set	messages: + **msg389639**
2021-03-28 17:57:13	milanjugessur1404	set	nosy: + **milanjugessur1404** messages: + **msg389638**
2021-02-22 19:27:16	Alexander Riccio	set	messages: + **msg387537**
2021-02-22 19:18:31	christian.heimes	set	nosy: + **christian.heimes** messages: + **msg387536**
2021-02-22 19:09:13	Alexander Riccio	set	nosy: + **Alexander Riccio** messages: + **msg387535**
2021-02-17 22:34:33	vstinner	set	messages: + **msg387194** title: [security] ctypes double representation BoF -> [security][CVE-2021-3177] ctypes double representation BoF
2021-01-18 22:29:08	vstinner	set	messages: + **msg385236**
2021-01-18 21:34:26	ned.deily	set	keywords: + **security_issue** priority: normal -> high versions: + Python 3.6, Python 3.7, Python 3.8, Python 3.9
2021-01-18 21:29:34	benjamin.peterson	set	messages: + **msg385234**
2021-01-18 21:28:57	benjamin.peterson	set	messages: + **msg385233**
2021-01-18 21:24:05	benjamin.peterson	set	messages: + **msg385231**
2021-01-18 21:11:52	benjamin.peterson	set	messages: + **msg385229**
2021-01-18 20:51:14	benjamin.peterson	set	pull_requests: + **pull_request23072**
2021-01-18 20:49:42	benjamin.peterson	set	pull_requests: + **pull_request23071**
2021-01-18 20:47:38	miss-islington	set	pull_requests: + **pull_request23070**
2021-01-18 20:47:25	miss-islington	set	nosy: + **miss-islington** pull_requests: + **pull_request23069**
2021-01-18 20:47:22	benjamin.peterson	set	status: open -> closed resolution: fixed messages: + **msg385226** stage: patch review -> resolved
2021-01-18 15:29:01	benjamin.peterson	set	keywords: + **patch** nosy: + **benjamin.peterson** pull_requests: + **pull_request23061** stage: patch review
2021-01-18 14:52:45	vstinner	set	nosy: + **vstinner** title: ctypes double representation BoF -> [security] ctypes double representation BoF
2021-01-16 08:03:27	JordyZomer	create	