homepage

search open all

- Python Home
- About
- News
- Documentation
- Downloads
- Community
- Foundation
- Developer's Guide
- Issue Tracker
  - **Issues**
    - Search
    - Random Issue
    - Show issue:
  - **Summaries**
    - Issues with patch
    - Easy issues
    - Stats
  - **User**
    - Login
      Remember me?
      Login
    - Lost your login?
  - **Administration**
    - User List
    - Committer List
  - **Help**
    - Tracker Documentation
    - Tracker Development
    - Report Tracker Problem

Issue41944

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/86110

classification

| | | | |
|---|---|---|---|
| **Title:** | [security][CVE-2020-27619] Python testsuite calls eval() on content received via HTTP | | |
| **Type:** | security | **Stage:** | resolved |
| **Components:** | Tests | **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:** | The Compiler, miss-islington, ned.deily, pablogsal, serhiy.storchaka, vstinner, zach.ware |
| **Priority:** | normal | **Keywords:** | patch, security_issue |

Created on **2020-10-05 14:40** by **serhiy.storchaka**, last changed **2022-04-11 14:59** by **admin**. This issue is now **closed**.

**Pull Requests**

| URL | Status | Linked | Edit |
|---|---|---|---|
| PR 22566 | merged | serhiy.storchaka, 2020-10-05 14:49 | |
| PR 22575 | merged | The Compiler, 2020-10-06 10:45 | |
| PR 22576 | merged | miss-islington, 2020-10-06 12:15 | |
| PR 22577 | merged | miss-islington, 2020-10-06 12:15 | |
| PR 22578 | merged | miss-islington, 2020-10-06 12:38 | |
| PR 22579 | merged | miss-islington, 2020-10-06 12:38 | |

**Messa**

**msg378036** - **(view)** **Author: Serhiy Storchaka (serhiy.storcl**

As was reported by Florian Bruhin, Python testsuite calls eval() on content received via HTTP (in Lib/test/multibytecodec_support.py).

**msg378104** - **(view)** **Author: Florian Bruhin (**

I wonder if I should request a CVE for this as well? Just to make sure the word gets out to distributions/organizations/etc. running the Pyth

**msg378105** - (view) **Author: STINNER Victor (vstinner**

I don't think that a CVE is justified.

I don't know anyone running the Python test suite on production. Only developers of Python itself run Python.

**msg378106** - (view) **Author: STINNER Victor (vstinner**

Oops: Only developers of Python itself run the Python test suite.

**msg378107** - (view) **Author: Florian Bruhin (**

That assumption is false. For starters, distribution packagers do:

https://github.com/archlinux/svntogit-packages/blob/3fc85177e35d1ff9ab000950c5d1af9567730434/trunk/PKGBUILD#L72-L84

https://src.fedoraproject.org/rpms/python3.9/blob/master/f/python3.9.spec#_1168

When I build a Python from source (via an Arch User Repository package), I do as well, and so does anyone installing those packages by defaul

Anyone building with --enable-optimizations (PGO) will likely do so as well, though I'm not sure if that runs this part of the testsuite.

**msg378108** - (view) **Author: STINNER Victor (vstinner**

I'm not saying that this issue is not a vulnerability, just that the scope is limited.

By default, downloaded from the Internet are disabled. You have to opt-in for that using -u network (or -u all which enables the network resc

Impacted:

* "make testall", "make testuniversal" and "make buildbottest" commands are impacted (pass -u all to the test suite).

* Python buildbot workers are impacted: they run the "make buildbottest" command.

* Travis CI is impacted: it runs "./python -m test -uall,-cpu (...)".

* Multiple GitHub Action jobs are impacted (coverage, Windows, macOS, Ubuntu): run "-uall,-cpu".

* Azure Pipelines jobs are impacted: use -uall,-cpu.

> https://src.fedoraproject.org/rpms/python3.9/blob/master/f/python3.9.spec#_1168

Fedora packages are not impacted: no -u option is passed to the test suite.

> Anyone building with --enable-optimizations (PGO) will likely do so as well, though I'm not sure if that runs this part of the testsuite.

PGO build is not impacted, it uses "./python -m test --pgo" (download is disabled). Moreover, multibyte codec checks are not run by this comm

**msg378110** - (view) **Author: Florian Bruhin (**

Thanks for the clarification - I wasn't aware those tests aren't run by default.

FWIW I found another place where a similar thing is done, though by chance it's probably not exploitable - see GH-22575.

**msg378111** - (view) **Author: STINNER Victor (vstinner**

> FWIW I found another place where a similar thing is done, though by chance it's probably not exploitable - see GH-22575.

I agree that test_ucn is not exploitable, but it would be nice to harden it anyway.

Extract of the code:

```
            self.assertEqual(unicodedata.lookup(seqname), codepoints)
            with self.assertRaises(SyntaxError):
                self.checkletter(seqname, None)
```

test_ucn downloads http://www.pythontest.net/unicode/13.0.0/NamedSequences.txt and calls checkletter() on each line, but first it ensures tha

I don't see how it would be possible to inject arbitrary Python code in the 'seqname' variable without making unicodedata.lookup() to fail.

**msg378114** - (view) **Author: STINNER Victor (vstinner**

I'm now tracking this vulnerability at:
https://python-security.readthedocs.io/vuln/cjk-codec-download-eval.html

**msg378117** - (view) **Author: Serhiy Storchaka (serhiy.storch**

New changeset 2ef5caa58febc8968e670e39e3d37cf8eef3cab8 by Serhiy Storchaka in branch 'master':
bpo-41944: No longer call eval() on content received via HTTP in the CJK codec tests (GH-22566)
https://github.com/python/cpython/commit/2ef5caa58febc8968e670e39e3d37cf8eef3cab8

**msg378118** - (view) **Author: miss-islington (**

New changeset b664a1df4ee71d3760ab937653b10997081b1794 by Miss Skeleton (bot) in branch '3.9':
bpo-41944: No longer call eval() on content received via HTTP in the CJK codec tests (GH-22566)
https://github.com/python/cpython/commit/b664a1df4ee71d3760ab937653b10997081b1794

**msg378119** - (view) **Author: STINNER Victor (vstinner**

New changeset 6c6c256df3636ff6f6136820afaefa5a10a3ac33 by Miss Skeleton (bot) in branch '3.8':
bpo-41944: No longer call eval() on content received via HTTP in the CJK codec tests (GH-22566) (GH-22577)
https://github.com/python/cpython/commit/6c6c256df3636ff6f6136820afaefa5a10a3ac33

**msg378120 - (view)** **Author: STINNER Victor (vstinner**

Since it's a security vulnerability, I created backports to 3.6 and 3.7 as well.

**msg378125 - (view)** **Author: STINNER Victor (vstinner**

New changeset a8bf44d04915f7366d9f8dfbf84822ac37a4bab3 by Florian Bruhin in branch 'master':
bpo-41944: No longer call eval() on content received via HTTP in the UnicodeNames tests (GH-22575)
https://github.com/python/cpython/commit/a8bf44d04915f7366d9f8dfbf84822ac37a4bab3

**msg379082 - (view)** **Author: Ned Deily (ned.deily) ***

New changeset 43e523103886af66d6c27cd72431b5d9d14cd2a9 by Miss Skeleton (bot) in branch '3.7':
bpo-41944: No longer call eval() on content received via HTTP in the CJK codec tests (GH-22566) (GH-22578)
https://github.com/python/cpython/commit/43e523103886af66d6c27cd72431b5d9d14cd2a9

**msg379085 - (view)** **Author: Ned Deily (ned.deily) ***

New changeset e912e945f2960029d039d3390ea08835ad39374b by Miss Skeleton (bot) in branch '3.6':
bpo-41944: No longer call eval() on content received via HTTP in the CJK codec tests (GH-22566) (GH-22579)
https://github.com/python/cpython/commit/e912e945f2960029d039d3390ea08835ad39374b

**msg379713 - (view)** **Author: STINNER Victor (vstinner**

Thanks for the fix Serhiy and thanks Florian Bruhin for the bug report!

**msg380319 - (view)** **Author: STINNER Victor (vstinner**

The CVE-2020-27619 has been assigned to this issue.

**msg380320 - (view)** **Author: STINNER Victor (vstinner**

Red Hat advisory: https://access.redhat.com/security/cve/CVE-2020-27619

**History**

| Date | User | Action | Args |
|---|---|---|---|
| 2022-04-11 14:59:36 | admin | set | github: 86110 |
| 2020-11-04 13:09:52 | vstinner | set | messages: + msg380320 |
| 2020-11-04 13:09:32 | vstinner | set | messages: + msg380319<br>title: [security] Python testsuite calls eval() on content received via HTTP -> [security][CVE-2020-27619] Python testsuite calls eval() on content received via HTTP |
| 2020-10-27 02:25:42 | vstinner | set | messages: + msg379713 |
| 2020-10-20 04:47:52 | ned.deily | set | keywords: + security_issue<br>status: open -> closed<br>stage: patch review -> resolved<br>resolution: fixed<br>versions: + Python 3.6, Python 3.7 |
| 2020-10-20 04:46:17 | ned.deily | set | messages: + msg379085 |
| 2020-10-20 02:38:43 | ned.deily | set | nosy: + ned.deily<br>messages: + msg379082 |
| 2020-10-06 14:22:06 | vstinner | set | messages: + msg378125 |
| 2020-10-06 12:39:20 | vstinner | set | messages: + msg378120 |
| 2020-10-06 12:38:57 | vstinner | set | messages: + msg378119 |
| 2020-10-06 12:38:19 | miss-islington | set | pull_requests: + pull_request21574 |
| 2020-10-06 12:38:07 | miss-islington | set | pull_requests: + pull_request21573 |
| 2020-10-06 12:37:44 | miss-islington | set | messages: + msg378118 |
| 2020-10-06 12:15:21 | miss-islington | set | pull_requests: + pull_request21572 |
| 2020-10-06 12:15:11 | miss-islington | set | nosy: + miss-islington<br>pull_requests: + pull_request21571 |
| 2020-10-06 12:14:59 | serhiy.storchaka | set | messages: + msg378117 |
| 2020-10-06 11:07:40 | vstinner | set | messages: + msg378114 |
| 2020-10-06 10:55:47 | vstinner | set | messages: + msg378111 |

| | | | |
|---|---|---|---|
| 2020-10-06 10:47:19 | The Compiler | set | messages: + msg378110 |
| 2020-10-06 10:45:56 | The Compiler | set | pull_requests: + pull_request21570 |
| 2020-10-06 10:28:20 | vstinner | set | nosy: + zach.ware, pablogsal<br>messages: + msg378108 |
| 2020-10-06 09:42:03 | The Compiler | set | messages: + msg378107 |
| 2020-10-06 09:25:14 | vstinner | set | messages: + msg378106 |
| 2020-10-06 09:24:54 | vstinner | set | messages: + msg378105<br>title: Python testsuite calls eval() on content received via HTTP -> [security] Python testsuite calls eval() on content received via HTTP |
| 2020-10-06 09:15:43 | The Compiler | set | messages: + msg378104 |
| 2020-10-05 14:49:59 | serhiy.storchaka | set | keywords: + patch<br>stage: patch review<br>pull_requests: + pull_request21561 |
| 2020-10-05 14:40:52 | serhiy.storchaka | create | |

Supported by The Python Software Foundation,
Powered by Roundup
Copyright © 1990-2022, Python Software Foundation
Legal Statements