

[New issue](#)[Jump to bottom](#)

Slow IDNA decoding with large strings [CVE-2022-45061]

#98433

Closed

guidovranken opened this issue on Oct 19 · 4 comments

Labels

[3.7](#)[3.8](#)[3.9](#)[3.10](#)[3.11](#)[3.12](#)[type-bug](#)[type-security](#)

guidovranken commented on Oct 19 • edited by bedevere-bot ▼

Bug report

Originally reported to the security address on September 9.

```
('xn--016c'+ 'a'*5000).encode('utf-8').decode('idna')
```

The execution time is not linear in relation to the input string size, which can cause slowness with large inputs:

10 chars = 0.016 seconds

100 chars = 0.047 seconds

1000 chars = 2.883 seconds

2500 chars = 17.724 seconds

5000 chars = 1 min 10 seconds

Comment by @tiran:

According to spec <https://unicode.org/reports/tr46/> an IDNA label must not be longer than 63 characters. Python's idna module enforces the restriction, but too late.

This may be abused in some cases, for example by passing a crafted host name to `asyncio.create_connection`:

```
import asyncio
```



```
async def main():
    loop = asyncio.get_running_loop()

    await loop.create_connection(
        lambda: [], ('xn--016c'+ 'a'*5000).encode('utf-8'), 443
    )

asyncio.run(main())
```

Your environment

- CPython versions tested on: CPython repository 'main' branch checkout, version 3.8.12, version 2.7.18
- Operating system and architecture: Ubuntu Linux x64
- PR: [gh-98433: Fix quadratic time idna decoding.](#) #99092
- PR: [\[3.11\] gh-98433: Fix quadratic time idna decoding. \(GH-99092\)](#) #99222
- PR: [\[3.10\] gh-98433: Fix quadratic time idna decoding. \(GH-99092\) \(GH-99222\)](#) #99229
- PR: [\[3.9\] gh-98433: Fix quadratic time idna decoding. \(GH-99092\) \(GH-99222\)](#) #99230
- PR: [\[3.8\] gh-98433: Fix quadratic time idna decoding. \(GH-99092\) \(GH-99222\)](#) #99231
- PR: [\[3.7\] gh-98433: Fix quadratic time idna decoding. \(GH-99092\) \(GH-99222\)](#) #99232

  **guidovranken** added the **type-bug** label on Oct 19

  **pochmann** mentioned this issue 22 days ago

Exponential IDNA codec decoding potential denial of service #99083

 Closed

  **gpshead** added **type-security** **3.11** **3.10** **3.9** **3.8** **3.12** labels 22 days ago

gpshead commented 22 days ago

Member

This is probably in `ToUnicode` and `ToASCII` of <https://github.com/python/cpython/blob/main/Lib/encodings/idna.py> and/or in <https://github.com/python/cpython/blob/main/Lib/encodings/punycode.py> itself, where we could presumably just do an up front length check and reject inputs that are obviously too long to possibly decode into a label length that DNS standards will accept.

If there are libraries that allow an attacker controlled hostname without a reasonable length check on it to get into a connect or similar call that tries idna decoding, that'd make this remotely exploitable. Based solely on code inspection, the `urllib.request.HTTPRedirectHandler` class is *probably* vulnerable to this - <https://github.com/python/cpython/blob/main/Lib/urllib/request.py#L652> - the location or uri headers it consumes on a HTTP 302 redirect response to construct the new URL are not obviously limited, nor is the host that ultimately winds it way down into the socket module. (I didn't test this, I was just reading code) A test case would be to point urllib at a malicious server that sends a 2000 byte idna hostname in a 302 redirect header...

vstinner commented 22 days ago

Member

The issue [#99083](#) was marked as a duplicate of this issue.

 **gpshead** added a commit to `gpshead/cpython` that referenced this issue 22 days ago

 [pythonGH-98433](#): Fix quadratic time idna decoding. ...

✓ 365a6cb

  **bedevere-bot** mentioned this issue 22 days ago

gh-98433: Fix quadratic time idna decoding. #99092

 Merged

 2 tasks

 **gpshead** added a commit that referenced this issue 18 days ago

 [gh-98433](#): Fix quadratic time idna decoding. ([#99092](#)) ...

✗ d315722

 **miss-islington** pushed a commit to `miss-islington/cpython` that referenced this issue 18 days ago

 [pythonGH-98433](#): Fix quadratic time idna decoding. ([pythonGH-99092](#)) ...

3a692f2

  **bedevere-bot** mentioned this issue 18 days ago

[3.11] gh-98433: Fix quadratic time idna decoding. (GH-99092) #99222

 Merged

 **gpshead** added a commit that referenced this issue 18 days ago

 [\[3.11\] gh-98433](#): Fix quadratic time idna decoding. ([GH-99092](#)) ([#99222](#)) ...

✗ a6f6c3a

 This was referenced 18 days ago

[3.10] [gh-98433](#): Fix quadratic time idna decoding. (GH-99092) (GH-99222) #99229

 Merged

[3.9] [gh-98433](#): Fix quadratic time idna decoding. (GH-99092) (GH-99222) #99230

 Merged

 **miss-islington** added a commit to miss-islington/cpython that referenced this issue 18 days ago



[3.11] [pythongh-98433](#): Fix quadratic time idna decoding. ([pythonGH-99092](#) ...

✓ da895b6

 This was referenced 18 days ago

[3.8] [gh-98433](#): Fix quadratic time idna decoding. (GH-99092) (GH-99222) #99231

 Merged

[3.7] [gh-98433](#): Fix quadratic time idna decoding. (GH-99092) (GH-99222) #99232

 Merged

 **miss-islington** added a commit to miss-islington/cpython that referenced this issue 18 days ago



[3.11] [pythongh-98433](#): Fix quadratic time idna decoding. ([pythonGH-99092](#) ...


✓ b8f8994

 **miss-islington** added a commit to miss-islington/cpython that referenced this issue 18 days ago



[3.11] [pythongh-98433](#): Fix quadratic time idna decoding. ([pythonGH-99092](#) ...

✓ fa792dd

  **gpshead** added the 3.7 label 18 days ago

 **ned-deily** pushed a commit that referenced this issue 18 days ago



[3.7] [gh-98433](#): Fix quadratic time idna decoding. ([GH-99092](#)) ([GH-99232](#)) ...

✗ b0b590b

 **miss-islington** added a commit that referenced this issue 18 days ago



[3.11] [gh-98433](#): Fix quadratic time idna decoding. ([GH-99092](#)) ([GH-99222](#)) ...

✗ 9bb8e18

gpshead commented 17 days ago

Member

PRs are either merged or will be merged before the next release (marked as release-blockers) so I'm closing this.

A CVE id has been assigned [CVE-2022-45061](#) for tracking purposes.



gpshead closed this as completed 17 days ago



gpshead changed the title ~~Slow IDNA decoding with large strings~~ Slow IDNA decoding with large strings [CVE-2022-45061] 17 days ago

vstinner commented 17 days ago

Member

I created <https://python-security.readthedocs.io/vuln/slow-idna-large-strings.html> to track this vulnerability. The fix is not merged into 3.8 and 3.9 branches yet.



ambv pushed a commit that referenced this issue 16 days ago



[3.8] [gh-98433](#): Fix quadratic time idna decoding. ([GH-99092](#)) ([GH-99222](#))...

✓ 82ca283



ambv pushed a commit that referenced this issue 16 days ago



[3.9] [gh-98433](#): Fix quadratic time idna decoding. ([GH-99092](#)) ([GH-99222](#))...

✓ c09dba5



halstead pushed a commit to openembedded/openembedded-core that referenced this issue 3 days ago



python3: Fix [CVE-2022-45061](#) ...

4498ca9

Assignees

No one assigned

Labels

3.7 3.8 3.9 3.10 3.11 3.12 type-bug type-security

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

