» Issue32981

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/77162

classification

Title:	Catastrophic backtracking in poplib (CVE-2018-1060) and difflib (CVE-2018-1061)		
Type:	security	**Stage**:	resolved
Components:	Library (Lib)	**Versions**:	Python 3.8, Python 3.7, Python 3.6, Python 3.4, Python 3.5, Python 2.7

process

Status:	closed	**Resolution**:	fixed
Dependencies:		**Superseder**:	
Assigned To:		**Nosy List**:	benjamin.peterson, davisjam, larry, ned.deily, tim.peters, vstinner
Priority:	critical	**Keywords**:	patch, security_issue

Created on **2018-03-02 00:36** by **davisjam**, last changed **2022-04-11 14:58** by **admin**. This issue is now **closed**.

Pull Requests

URL	Status	Linked	Edit
PR 5955	merged	davisjam, 2018-03-02 00:36	
PR 5969	merged	miss-islington, 2018-03-04 05:33	
PR 5970	merged	benjamin.peterson, 2018-03-04 05:44	
PR 5971	merged	benjamin.peterson, 2018-03-04 05:47	
PR 6034	merged	ned.deily, 2018-03-08 20:00	
PR 6035	closed	ned.deily, 2018-03-08 20:02	

Messages (10)

msg313119 - (view) **Author: James Davis (davisjam) *** **Date: 2018-03-02 00:36**

```
Hi Python security team,

My name is James Davis. I'm a security researcher at Virginia Tech.

The python core (cpython) has 2 regular expressions vulnerable to catastrophic
```

```
backtracking that look like potential DOS vectors.
The vulnerable expressions are listed below.

Each vulnerability has the following keys, explained in more detail below:
 - pattern
 - filesIn (as of December/January; I excluded any appearances in irrelevant-
looking dirs, and in '.min' files)
 - stringLenFor10Sec
 - nPumpsFor10Sec
 - attackFormat
 - blowupCurve

The attack format describes how to generate an attack string.
On my machine, an attack string generated using nPumpsFor10Sec repetitions
("pumps") of the pump string(s)
blocks the python regex engine for 10 seconds, though this will vary based on
your hardware.

Compose an attack string like this:
  'prefix 1' + 'pump 1' X times + 'prefix 2' + 'pump 2' X times + ... + suffix
Example:
  With pumpPairs: [{'prefix': 'a', 'pump': 'b'}], suffix: 'c', an attack string
with three pumps would be:
    abbbc

Catastrophic backtracking blows up at either an exponential rate or a super-
linear (power law) rate.
The blowupCurve indicates how severe the blow-up is.
The 'type' is either EXP(onential) or POW(er law) in the number of pumps (x).
The 'parms' are the parameters for the two curve types. The second parameter is
more important, because:
  EXP: f(x) = parms[0] * parms[1]^x
  POW: f(x) = parms[0] * x^parms[1]

JSON formatted:

Vuln 1:

{
   "attackFormat" : {
      "pumpPairs" : [
         {
            "pump" : "<a",
            "prefix" : "+OKa"
         }
      ],
      "suffix" : "+"
   },
   "blowupCurve" : {
      "parms" : [
         2.71096268836868e-08,
         1.83422078906374
      ],
      "type" : "POWER",
      "r2" : 0.997503282766243
```

```
   },
   "stringLenFor10Sec" : 96655,
   "nPumpsFor10Sec" : "48325",
   "pattern" : "\\+OK.*(<[^>]+>)",
   "filesIn" : [
      [
         "Lib/poplib.py"
      ]
   ]
}

Vuln 2:

{
   "blowupCurve" : {
      "parms" : [
         1.31911634447601e-08,
         1.89691808610459
      ],
      "r2" : 0.998387790742004,
      "type" : "POWER"
   },
   "stringLenFor10Sec" : 48328,
   "attackFormat" : {
      "pumpPairs" : [
         {
            "pump" : "\t",
            "prefix" : "\t"
         }
      ],
      "suffix" : "##"
   },
   "pattern" : "\\s*#?\\s*$",
   "filesIn" : [
      [
         "Lib/difflib.py"
      ]
   ],
   "nPumpsFor10Sec" : "48325"
}
```

msg313198 - (view) **Author: Benjamin Peterson (benjamin.peterson) *** **Date: 2018-03-04 05:33**

New changeset **0e6c8ee2358a2e23117501826c008842acb835ac** by Benjamin Peterson (Jamie Davis) in branch 'master':
~~**bpo-32981**~~: Fix catastrophic backtracking vulns (~~**#5955**~~)
https://github.com/python/cpython/commit/0e6c8ee2358a2e23117501826c008842acb835ac

msg313200 - (view) **Author: Benjamin Peterson (benjamin.peterson) *** **Date: 2018-03-04 05:55**

New changeset **0902a2d6b2d1d9dbde36aeaaccf1788ceaa97143** by Benjamin Peterson (Miss Islington (bot)) in branch '3.7':
~~**bpo-32981**~~: Fix catastrophic backtracking vulns (**GH-5955**)
https://github.com/python/cpython/commit/0902a2d6b2d1d9dbde36aeaaccf1788ceaa97143

msg313202 - (view) **Author: Benjamin Peterson (benjamin.peterson) *** **Date: 2018-03-04 06:18**

New changeset **e052d40cea15f582b50947f7d906b39744dc62a2** by Benjamin Peterson in branch '2.7':
[2.7] ~~**bpo-32981**~~: Fix catastrophic backtracking vulns (**GH-5955**)
https://github.com/python/cpython/commit/e052d40cea15f582b50947f7d906b39744dc62a2

msg313203 - (view) **Author: Benjamin Peterson (benjamin.peterson) *** **Date: 2018-03-04 06:59**

New changeset **c9516754067d71fd7429a25ccfcb2141fc583523** by Benjamin Peterson in branch '3.6':
[3.6] ~~**bpo-32981**~~: Fix catastrophic backtracking vulns (**GH-5955**)
https://github.com/python/cpython/commit/c9516754067d71fd7429a25ccfcb2141fc583523

msg313609 - (view) **Author: Larry Hastings (larry) *** **Date: 2018-03-11 18:28**

New changeset **942cc04ae44825ea120e3a19a80c9b348b8194d0** by larryhastings (Ned Deily) in branch '3.4':
[3.4] ~~**bpo-32981**~~: Fix catastrophic backtracking vulns (**GH-5955**) (~~**#6035**~~)
https://github.com/python/cpython/commit/942cc04ae44825ea120e3a19a80c9b348b8194d0

msg313610 - (view) **Author: Larry Hastings (larry) *** **Date: 2018-03-11 18:29**

New changeset **937ac1fe069a4dc8471dff205f553d82e724015b** by larryhastings (Ned Deily) in branch '3.5':
[3.5] ~~**bpo-32981**~~: Fix catastrophic backtracking vulns (**GH-5955**) (~~**#6034**~~)
https://github.com/python/cpython/commit/937ac1fe069a4dc8471dff205f553d82e724015b

msg313611 - (view) **Author: Larry Hastings (larry) *** **Date: 2018-03-11 18:29**

Is this ready to close?

msg313803 - (view) **Author: Ned Deily (ned.deily) *** **Date: 2018-03-14 05:23**

> Is this ready to close?

The fixes are now available from the cpython repo for all current security and maintenance branches (3.4 to 3.7 plus 2.7). They are now released in 3.6.5rc1 and will be available in the next releases of other branches: 3.7.0, 3.5.6, 3.4.9, and 2.7.15.

Thanks again for reporting the issues, James, and helping to resolve them!

msg316124 - (view) **Author: STINNER Victor (vstinner) *** **Date: 2018-05-03 14:14**

FYI I tracked this vulnerability at:
http://python-security.readthedocs.io/vuln/cve-2018-1060_difflib_and_poplib_catastrophic_backtracking.html

History

Date	User	Action	Args
2022-04-11 14:58:58	admin	set	github: 77162

2019-05-10 18:09:12	ned.deily	set	messages: - **msg342092**
2019-05-10 17:36:38	ned.deily	set	messages: + **msg342092**
2018-05-03 14:14:56	vstinner	set	nosy: + **vstinner** messages: + **msg316124**
2018-03-14 05:23:09	ned.deily	set	status: open -> closed nosy: + **ned.deily** messages: + **msg313803** resolution: fixed stage: patch review -> resolved
2018-03-11 18:29:43	larry	set	messages: + **msg313611**
2018-03-11 18:29:08	larry	set	messages: + **msg313610**
2018-03-11 18:28:55	larry	set	messages: + **msg313609**
2018-03-08 20:20:10	ned.deily	set	nosy: + **larry** title: Catastrophic backtracking in poplib and difflib -> Catastrophic backtracking in poplib (CVE-2018-1060) and difflib (CVE-2018-1061) priority: normal -> critical versions: + Python 2.7, Python 3.4, Python 3.5, Python 3.6, Python 3.7, Python 3.8 keywords: + **security_issue**
2018-03-08 20:02:17	ned.deily	set	pull_requests: + **pull_request5797**
2018-03-08 20:00:01	ned.deily	set	pull_requests: + **pull_request5796**
2018-03-04 06:59:15	benjamin.peterson	set	messages: + **msg313203**
2018-03-04 06:18:19	benjamin.peterson	set	messages: + **msg313202**
2018-03-04 05:55:09	benjamin.peterson	set	messages: + **msg313200**
2018-03-04 05:47:22	benjamin.peterson	set	pull_requests: + **pull_request5737**
2018-03-04 05:44:44	benjamin.peterson	set	pull_requests: + **pull_request5736**
2018-03-04 05:33:43	miss-islington	set	keywords: + **patch** stage: patch review pull_requests: + **pull_request5735**
2018-03-04 05:33:36	benjamin.peterson	set	nosy: + **benjamin.peterson** messages: + **msg313198**
2018-03-02 05:04:09	rhettinger	set	nosy: + **tim.peters**
2018-03-02 00:36:19	davisjam	create	