urllib basic auth regex denial of service

The AbstractBasicAuthHandler class of the urllib.request module uses an inefficient regular expression (catastrophic backtracking) which can be exploited by an attacker to cause a denial of service.

See also https://bugs.python.org/issue43075

Dates:

- Disclosure date: **2019-11-17** (Python issue bpo-38826 reported)
- Reported at: 2019-11-17 (bpo-38826)
- Reported by: Ben Caller and Matt Schwager

Fixed In

- Python **3.5.10** (2020-09-05) fixed by commit 37fe316 (branch 3.5) (2020-06-20)
- Python **3.6.11** (2020-06-27) fixed by commit 69cdeeb (branch 3.6) (2020-04-03)
- Python **3.7.8** (2020-06-27) fixed by commit b57a736 (branch 3.7) (2020-04-02)
- Python **3.8.3** (2020-05-13) fixed by commit ea9e240 (branch 3.8) (2020-04-02)
- Python **3.9.0** (2020-10-05) fixed by commit 0b297d4 (branch 3.9) (2020-04-02)

Python issue

Regular Expression Denial of Service in urllib.request.AbstractBasicAuthHandler.

- Python issue: bpo-38826
- Creation date: 2019-11-17
- Reporter: Ben Caller

CVE-2020-8492

Python 2.7 through 2.7.17, 3.5 through 3.5.9, 3.6 through 3.6.10, 3.7 through 3.7.6, and 3.8 through 3.8.1 allows an HTTP server to conduct Regular Expression Denial of Service (ReDoS) attacks against a client because of urllib.request.AbstractBasicAuthHandler catastrophic backtracking.

- CVE ID: CVE-2020-8492
- Published: 2020-01-30
- CVSS Score: 7.1

Timeline

Timeline using the disclosure date **2019-11-17** as reference:

- 2019-11-17: Reported (bpo-38826)
- 2019-11-17: Python issue bpo-38826 reported by Ben Caller
- 2020-01-30 (**+74 days**): CVE-2020-8492 published
- 2020-04-02 (**+137 days**): commit 0b297d4 (branch 3.9)
- 2020-04-02 (**+137 days**): commit b57a736 (branch 3.7)
- 2020-04-02 (**+137 days**): commit ea9e240 (branch 3.8)
- 2020-04-03 (**+138 days**): commit 69cdeeb (branch 3.6)
- 2020-05-13 (**+178 days**): Python 3.8.3 released
- 2020-06-20 (**+216 days**): commit 37fe316 (branch 3.5)
- 2020-06-27 (**+223 days**): Python 3.6.11 released
- 2020-06-27 (**+223 days**): Python 3.7.8 released
- 2020-09-05 (**+293 days**): Python 3.5.10 released
- 2020-10-05: Python 3.9.0 released

Links

- https://bugs.python.org/issue39503