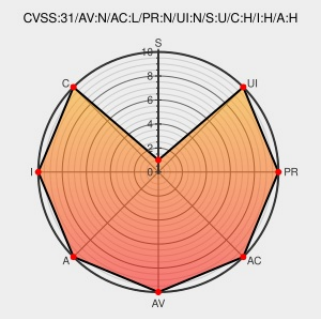
# CVE-2018-1000802

Published on: 09/18/2018 12:00:00 AM UTC

Last Modified on: 03/09/2023 07:15:00 PM UTC

## CVE-2018-1000802

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

Python Software Foundation Python (CPython) version 2.7 contains a CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in shutil module (make_archive function) that can result in Denial of service, Information gain via injection of arbitrary files on the system or entire drive. This attack appear to be exploitable via Passage of unfiltered user input to the function. This vulnerability appears to have been fixed in after commit add531a1e55b0a739b0f42582f1c9747e5649ace.

CVE-2018-1000802 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

### CVSS3 Score: 9.8 - CRITICAL

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | NONE | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | HIGH | HIGH | HIGH |

### CVSS2 Score: 7.5 - HIGH

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | PARTIAL | PARTIAL |

### CVE References

| Description | Tags | Link |
|---|---|---|

| | | |
|---|---|---|
| MEGA | Exploit<br>Third Party Advisory<br>mega.nz<br>text/html | MISC mega.nz/#!JUFiCC4R!mq-jQ8ySFwIhX6WMDujaZuNBfttDVt7DETIfOIQE1ig |
| [SECURITY] [DLA 1520-1] python3.4 security update | Mailing List<br>Third Party Advisory<br>lists.debian.org<br>text/html | MLIST [debian-lts-announce] 20180926 [SECURITY] [DLA 1520-1] python3.4 security update |
| Debian -- Security Information -- DSA-4306-1 python2.7 | Third Party Advisory<br>www.debian.org<br>Depreciated Link<br>text/html | DEBIAN DSA-4306 |
| [security-announce] openSUSE-SU-2020:0086-1: important: Security update | Mailing List<br>Third Party Advisory<br>lists.opensuse.org<br>text/html | SUSE openSUSE-SU-2020:0086 |
| Issue 34540: shutil._call_external_zip should use subprocess - Python tracker | Issue Tracking<br>Patch<br>Vendor Advisory<br>bugs.python.org<br>text/html | CONFIRM bugs.python.org/issue34540 |
| USN-3817-1: Python vulnerabilities \| Ubuntu security notices | Third Party Advisory<br>usn.ubuntu.com<br>text/html | UBUNTU USN-3817-1 |
| USN-3817-2: Python vulnerabilities \| Ubuntu security notices | Third Party Advisory<br>usn.ubuntu.com<br>text/html | UBUNTU USN-3817-2 |
| [2.7] closes bpo-34540: Convert shutil._call_external_zip to use subprocess rather than distutils.spawn. by benjaminp · Pull Request #8985 · python/cpython · GitHub | Patch<br>Vendor Advisory<br>github.com<br>text/html | CONFIRM github.com/python/cpython/pull/8985 |
| [SECURITY] [DLA 1519-1] python2.7 security update | Mailing List<br>Third Party Advisory<br>lists.debian.org<br>text/html | MLIST [debian-lts-announce] 20180925 [SECURITY] [DLA 1519-1] python2.7 security update |
| CVE-2018-1000802 Python Vulnerability in NetApp Products \| NetApp Product Security | security.netapp.com<br>text/html | CONFIRM security.netapp.com/advisory/ntap-20230309-0002/ |
| [2.7] closes bpo-34540: Convert shutil._call_external_zip to use subprocess rather than distutils.spawn. by benjaminp · Pull Request #8985 · python/cpython · | Patch<br>Vendor Advisory<br>github.com<br>text/html | CONFIRM github.com/python/cpython/pull/8985/commits/add531a1e55b0a739b0f42582f1c9747e5649a |

GitHub

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

## Exploit/POC from Github

### Python CVE-2018-1000802 Proof-of-Concept

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Canonical | Ubuntu Linux | 12.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 12.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Opensuse | Leap | 15.1 | All | All | All |
| Operating System | Opensuse | Leap | 15.1 | All | All | All |
| Application | Python | Python | All | All | All | All |
| Application | Python | Python | 2.7.0 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Python | Python | 2.7.0 | All | All | All |

- cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:
- cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:
- cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:
- cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:
- cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:
- cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:*:*:
- cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:*:*:
- cpe:2.3:a:python:python:*:*:*:*:*:*:*:*:
- cpe:2.3:a:python:python:2.7.0:*:*:*:*:*:*:*:
- cpe:2.3:a:python:python:2.7.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
|---|---|---|
| /r/AJsBotPlayground | [CRITICAL] CVE Report on March 10, 2023 12:14 | 2023-03-10 12:14:48 |
| /r/AJsBotPlayground | [CRITICAL] CVE Report on March 10, 2023 11:59 | 2023-03-10 11:59:25 |

← Previous ID

Next ID→

**CVE.report and Source URL Uptime Status status.cve.report**